RUGDOG

SMART CONTRACT SECURITY AUDIT

Final report

Plan: Simple

SECVSFOUR

June 2023

rugdog.net

the@rugdog.net

CONTENTS

INTRODUCTION

The report has been prepared for SECVSFOUR.

Rugdog has performed an $SECVSFOUR (SEC VS FOUR) project audit for its SEC(0x7f91beB2f51cB15760932b697b81cdF937BBa823) and FOUR(0x04255Ac99120a760609AD516992a05ACdF7Be624) token smart contracts. Both SEC and FOUR tokens are basic ERC20 tokens with capped supply of 44444444 fully minted during the deployment. Tokens are deployed on BSC network. PancakeSwap pairs are created for SEC/WBNB, FOUR/WBNB, and SEC/FOUR.

Name	SECVSFOUR
Audit date	2023-06-20 - 2023-06-20
Language	Solidity
Network	Binance Smart Chain

CONTRACTS CHECKED

Name	Address
FarmToken	0x04255Ac99120a760609AD516992a05ACdF7Be624, 0x7f91beB2f51cB15760932b697b81cdF937BBa823
PancakePair	0x946b5Ac0C9737B613A3F02B0a0720fEDEA416cd3

AUDIT PROCESS

The code was audited by the team according to the following order:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual confirmation of all the issues found by the tools

Manual audit

- Thorough manual analysis of smart contracts for security vulnerabilities
- Smart contracts' logic check

ATTACKS CHECKED

Title	Check result
Unencrypted Private Data On-Chain	✓ passed
Code With No Effects	✓ passed
Message call with hardcoded gas amount	✓ passed
Typographical Error	✓ passed
DoS With Block Gas Limit	✓ passed
Presence of unused variables	✓ passed
Incorrect Inheritance Order	✓ passed
Requirement Violation	✓ passed
Weak Sources of Randomness from Chain Attributes	✓ passed
Shadowing State Variables	✓ passed

Incorrect Constructor Name	✓ passed
Block values as a proxy for time	✓ passed
Authorization through tx.origin	✓ passed
DoS with Failed Call	✓ passed
Delegatecall to Untrusted Callee	✓ passed
Use of Deprecated Solidity Functions	✓ passed
Assert Violation	✓ passed
State Variable Default Visibility	✓ passed
Reentrancy	✓ passed
Unprotected SELFDESTRUCT Instruction	✓ passed
Unprotected Ether Withdrawal	✓ passed
Unchecked Call Return Value	✓ passed
Floating Pragma	✓ passed
Outdated Compiler Version	✓ passed
Integer Overflow and Underflow	✓ passed
Function Default Visibility	✓ passed

OVERVIEW OF RELEVANCE LEVELS

High relevance Issues of high relevance may lead to losses of users' funds as well as changes of ownership of a contract or possible issues with the logic of the contract.
High-relevance issues require immediate attention and a response from the team.

Medium relevance While issues of medium relevance don't pose as high a risk as the high-relevance ones do, they can be just as easily exploited by the team or a malicious user, causing a contract failure and damaging the project's reputation in the process. Usually, these issues can be fixed if the contract is redeployed.
Medium-relevance issues require a response from the team.

Low relevance Issues of low relevance don't pose high risks since they can't cause damage to the functionality of the contract. However, it's still recommended to consider fixing them.

ISSUES

High relevance issues

No high relevance issues found

Medium relevance issues

No medium relevance issues found

Low relevance issues

1. Ownable minting (FarmToken)

The FarmToken token has an owner, who can mint up to the fixed cap. Both SEC and FOUR tokens are deployed fully minted to their caps (44444444 tokens).

✧ CONCLUSION

SECVSFOUR FarmToken, PancakePair contracts were audited. 1 low relevance issue was found.

✧ 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 RugDog 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 RugDog 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.
The rights to publish the results of this audit are exclusively retained by RugDog.

RUGDOG

WOOF!

🌐 rugdog.net

✉ the@rugdog.net