freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

StepZoro
$StepZ

29/04/2022

TABLE OF CONTENTS

DISCLAIMER

The information provided on this analysis document is only
for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results
of this audit.

The score and the result will stay on this project page information
on our website https://freshcoins.io
FreshCoins Team does not guarantees that a project will not sell off
team supply, or any other scam strategy (RUG or Honeypot etc)

INTRODUCTION

FreshCoins (Consultant) was contracted by **StepZoro** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x630a763Ae57FC62247ADb681F396BAE8DC7FD9C7

Network: Binance Smart Chain (BSC)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 29/04/2022

StepZoro
$StepZ

AUDIT OVERVIEW

98

Security Score

98 Static Scan
Automatic scanning for common vulnerabilities

98 ERC Scan
Automatic checks for ERC's conformance

0 High

0 Medium

0 Low

0 Optimizations

0 Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Passed
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Passed
8	Methods execution permissions	Passed
9	Exchange rate impact	Passed
10	Malicious Event	Passed
11	Scoping and Declarations	Passed
12	Uninitialized storage pointers	Passed
13	Design Logic	Passed
14	Safe Zeppelin module	Passed

OWNER PRIVILEGES

Contract owner can't mint tokens after initial contract deploy.

Contract owner can change poolWallet address

Current value:

poolWallet: 0xbe870f41814ab4c5b07338b0d3b3deb68009017d

```solidity
function setPoolWallet(address poolWallet_) external onlyOwner {
    poolWallet = poolWallet_;
}
```

Contract owner can change tax (with threshold)

```solidity
function setPoolReward(uint256 reward) external onlyOwner {
    require(reward <= 500, "Pancake swap limitation");
    _poolReward = reward;
}
```

Contract owner can exclude/include wallet from tax

```solidity
function excludeAddress(address account) external onlyOwner {
    isExcludedFromFee[account] = true;
    emit EventExcludeAddress(account);
}

function removeExcludedAddress(address account) external onlyOwner {
    delete isExcludedFromFee[account];
    emit EventRemoveExcludeAddress(account);
}
```

Contract owner can renounce ownership

```solidity
function renounceOwnership() public virtual onlyOwner {
    _setOwner(address(0));
}
```

Contract owner can transfer ownership

```solidity
function transferOwnership(address newOwner) public virtual onlyOwner {
    require(newOwner != address(0), "Ownable: new owner is the zero address");
    _setOwner(newOwner);
}
```

CONCLUSION AND ANALYSIS

Smart Contracts within the scope were manually reviewed and analyzed with static tools.

Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.

Found no issue during the first review.

TOKEN DETAILS

Details

Buy fees: N/A

Sell fees: 5%

Max TX: N/A

Max Sell: N/A

Honeypot Risk

Ownership: Owned

Blacklist: Not detected

Modify Max TX: Not detected

Modify Max Sell: Not detected

Disable Trading: Not detected

Rug Pull Risk

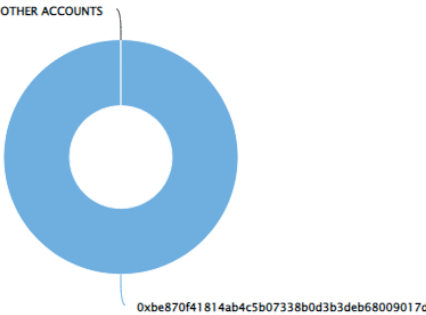Liquidity: N/A

Holders: Clean

STEPZORO TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (100,000,000,000.00 Tokens) of StepZoro | Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 1

StepZoro Top 10 Token Holders

Source: BscScan.com

OTHER ACCOUNTS

0xbe870f41814ab4c5b07338b0d3b3deb68009017d

(A total of 100,000,000,000.00 tokens held by the top 10 accounts from the total supply of 100,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xbe870f41814ab4c5b07338b0d3b3deb68009017d	100,000,000,000	100.0000%

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform.
The platform, its programming language, and other software related
to the smart contract can have its vulnerabilities that can lead to hacks.
The audit can't guarantee the explicit security of the
audited project / smart contract.