freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Zola
$ZOLA

09/02/2023

TOKEN OVERVIEW

Fees

• Buy fees: 7%

• Sell fees: 9%

Fees privileges

• Can't change fees

Ownership

• Owned

Minting

• No mint function

Max Tx Amount / Max Wallet Amount

• Can't change max tx amount or max wallet amount

Blacklist

• Blacklist function not detected

Other privileges

• Can exclude / include from fees

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 **Zola** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x85128F08ADEF4B50EABf262b4c9674d5ACEbe8F2

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 **09/02/2023**

AUDIT OVERVIEW

91

Security Score

89 Static Scan
Automatic scanning for common vulnerabilities

91 ERC Scan
Automatic checks for ERC's conformance

0 High

1 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't exclude an address from transactions**

● **Contract owner can exclude wallet from tax**

```
function setWhitelist(address _addr) external onlyOwner {
    _isFeeExempt[_addr] = true;
}
```

● **Contract owner can change rebase settings**

```
function setAutoRebase(bool _flag) external onlyOwner {
    if (_flag) {
        _autoRebase = _flag;
        _lastRebasedTime = block.timestamp;
    } else {
        _autoRebase = _flag;
    }
}
```

● **Contract owner can change treasuryReceiver, zolaRecoveryFundReceiver, pairAddress and pairContract addresses**

Current values:

treasuryReceiver: 0xa84bdb3a959c57c3aa71dbf6a2311b99ab05939a

zolaRecoveryFundReceiver: 0xc825cb917f3c19876255144b1620fb32b6f3dddd

pairAddress : 0x0bd0d928681989ce32bc099ec09bb5610b3fe40b

pairContract : 0x0bd0d928681989ce32bc099ec09bb5610b3fe40b

```
function setFeeReceivers(
    address _treasuryReceiver,
    address _zolaRecoveryFundReceiver
  ) external onlyOwner {
    treasuryReceiver = _treasuryReceiver;
    zolaRecoveryFundReceiver = _zolaRecoveryFundReceiver;
}

function setPairAddress(address _pairAddress) external onlyOwner {
    pairAddress = _pairAddress;
}

function setLP(address _address) external onlyOwner {
    pairContract = IPancakeSwapPair(_address);
}
```

● Contract owner can transfer ownership

```
function transferOwnership(address newOwner) external onlyOwner {
    _transferOwnership(newOwner);
}

function _transferOwnership(address newOwner) internal {
    require(newOwner != address(0));
    emit OwnershipTransferred(_owner, newOwner);
    _owner = newOwner;
}
```

● Contract owner can renounce ownership

```
function renounceOwnership() external onlyOwner {
    emit OwnershipRenounced(_owner);
    _owner = address(0);
}
```

Recommendation:

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. The risk can be prevented by temporarily locking the contract or renouncing ownership.

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 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	7%
Sell fees:	9%
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

Ownership:	Owned (By a Timelock Contract)
Blacklist:	Not detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

Rug Pull Risk

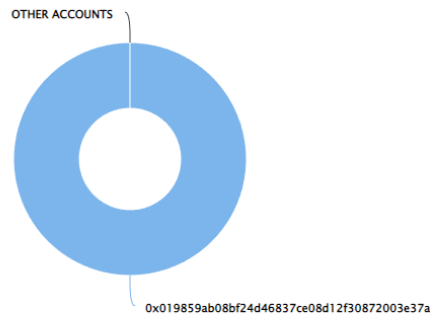|	
Liquidity:	N/A
Holders:	Clean

ZOLA TOKEN ANALYTICS
& TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (5,000,000.00 Tokens) of Zola | Token Total Supply: 5,000,000.00 Token | Total Token Holders: 1

Zola Top 10 Token Holders

Source: BscScan.com

OTHER ACCOUNTS

0x019859ab08bf24d46837ce08d12f30872003e37a

(A total of 5,000,000.00 tokens held by the top 10 accounts from the total supply of 5,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x019859ab08bf24d46837ce08d12f30872003e37a	5,000,000	100.0000%

● **Verified Token Contract:**
0x85128F08ADEF4B50EABf262b4c9674d5ACEbe8F2#code

● **Open Zeppelin Time-lock Controller:**
0x1878FCf431e1BD35F2e775965A001256Cfd7707f#code

● **Gnosis Multi-Sig Proposer of the Time-lock Controller:**
0xDDb347B2866cdF59B0964aD5e3fcCEf375BaFF70#code

● **Treasury Wallet:**
0xa84bdb3a959C57C3aa71DbF6a2311b99aB05939a#code

● **Recovery Fund Wallet:**
0xc825cb917F3C19876255144B1620fb32B6F3dDDd#code

● **Renouncing the admin rights of the Time lock Contract:**
0x46ebd9ce51eaa0139f523c00687d6657b7e54f9fc9f08b23012ec025dfc82220

● **Transferring the ownership of Zola Coin to the Time lock Contract:**
0x1ddbf58dde9b814a833ee623de4f47a1162060a58fe2b55fd8964b2ace4d2523

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.