freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

subZero

$zero

15/01/2022

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

0x88F5C723dB466f5cfB63598F3255562B1D82b442

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 15/01/2022

subZero
$zero

WEBSITE DIAGNOSTIC

https://subzerotoken.com/

0-49   **50-89**   **90-100**

92 Performance

90 Accessibility

100 Best Practices

74 SEO

NA Progressive Web App

Metrics

First Contentful Paint
1.0 s

Time to interactive
3.9 s

Speed Index
3.2 s

Total Blocking Time
230 ms

Large Contentful Paint
2.5 s

Cumulative Layout Shift
0

WEBSITE IMPROVEMENTS

Reduce unused JavaScript

Image elements do not have explicit width and height

Image elements do not have [alt] attributes

Background and foreground colors do not have a sufficient contrast ratio

Document does not have a meta description

AUDIT OVERVIEW

97

Security Score

96

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't exclude an address from transactions.

Contract owner can exclude/include wallet from reward

```solidity
function excludeFromReward(address account) public onlyOwner {
    // require(account != 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D, 'We can not exclude Uniswap router.');
    require(!_isExcluded[account], "Account is already excluded");
    if (_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}

function includeInReward(address account) external onlyOwner {
    require(_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

Contract owner can exclude/include wallet from fee

```solidity
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}
```

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");
    _transferOwnership(newOwner);
}
```

Contract owner can change the fees

```solidity
function setTaxFeePercent(uint256 taxFeeBps) external onlyOwner {
    require(taxFeeBps >= 0 && taxFeeBps <= 10**4, "Invalid bps");
    _taxFee = taxFeeBps;
}

function setLiquidityFeePercent(uint256 liquidityFeeBps)
    external
    onlyOwner
  {
    require(
      liquidityFeeBps >= 0 && liquidityFeeBps <= 10**4,
      "Invalid bps"
    );
    _liquidityFee = liquidityFeeBps;
}
```

Contract owner can change swap settings

```solidity
function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
    swapAndLiquifyEnabled = _enabled;
    emit SwapAndLiquifyEnabledUpdated(_enabled);
}
```

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: 5%

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

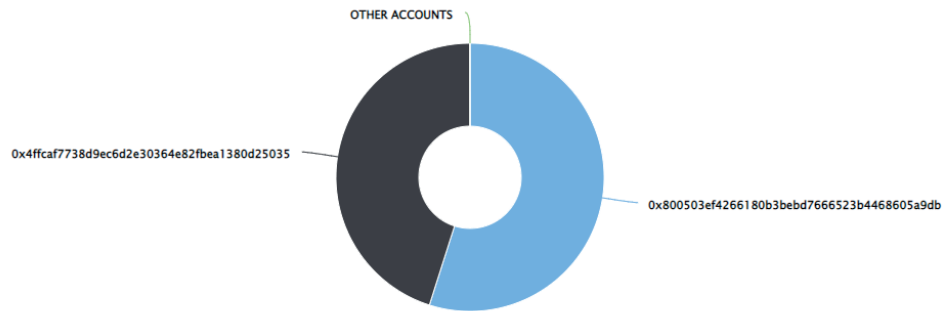## Rug Pull Risk

Liquidity: N/A

Holders: Clean

SUBZERO TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 2

subZero Top 10 Token Holders

Source: BscScan.com

OTHER ACCOUNTS

0x4ffcaf7738d9ec6d2e30364e82fbea1380d25035

0x800503ef4266180b3bebd7666523b4468605a9db

(A total of 1,000,000,000,000.00 tokens held by the top 10 accounts from the total supply of 1,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x800503ef4266180b3bebd7666523b4468605a9db	549,000,000,000	54.9000%
2	0x4ffcaf7738d9ec6d2e30364e82fbea1380d25035	451,000,000,000	45.1000%

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.