freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

VesTallyToken

$VTT

16/01/2022

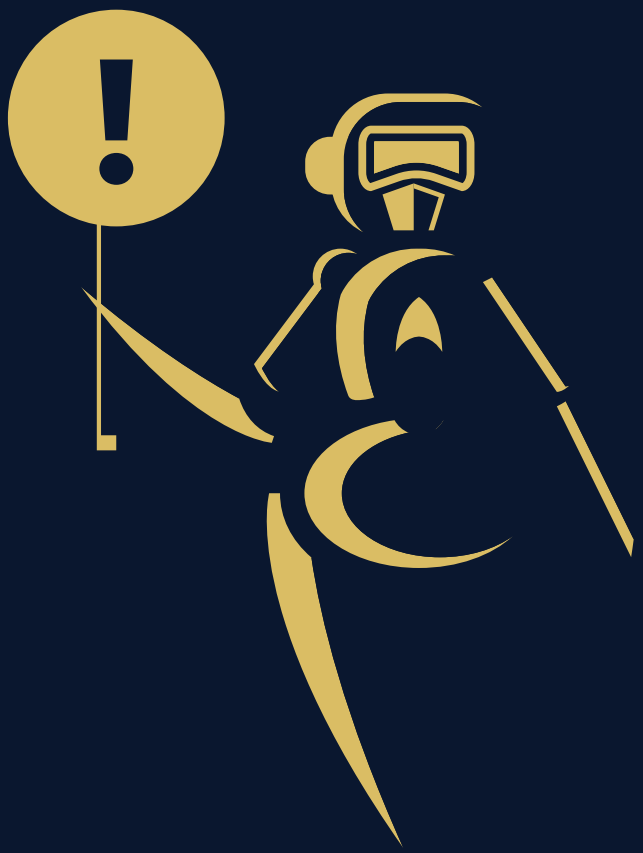
TABLE OF CONTENTS

DISCLAIMER

The information provided on this analysis decoument 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 VesTallyToken (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0xE34e3eDBc2964ac2B93034db83A9dc47A4E6E8Af

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 16/01/2022

WEBSITE DIAGNOSTIC

https://vestallytoken.com/

0-49 50-89 90-100

78	90	92	93	NA
Performance	Accessability	Best Practices	SEO	Progressive Web App

Metrics

First Contentful Paint
2.1 s

Time to interactive
17.4 s

Speed Index
6.4 s

Total Blocking Time
550 ms

Large Contentful Paint
2.7 s

Cumulative Layout Shift
0.023

Website Improvements

Reduce unused JavaScript

Eliminate render-blocking resources

Reduce unused CSS

Reduce initial server response time

Ensure text remains visible during webfont load

Avoid enormous network payloads Total size was 4,896 KiB

Background and foreground colors do not have a sufficient contrast ratio

AUDIT OVERVIEW

96

Security Score

94

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

```
function excludeFromReward(address account) public onlyOwner {
        require(!_isExcludedFromReward[account], "Account is already excluded");
        if(_rOwned[account] > 0) {
                _tOwned[account] = tokenFromReflection(_rOwned[account]);
        }
        _isExcludedFromReward[account] = true;
        _excludedFromReward.push(account);
}

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

Contract owner can exclude/include wallet from fee

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

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

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
        emit OwnershipTransferred(_owner, address(0));
        _owner = address(0);
}
```

Contract owner can transfer ownership

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

Contract owner can change the fees

```
function setRewardFeePercent(uint256 rewardFee) external onlyOwner {
        require(rewardFee <= 5, 'Tax exceeds maximum 5%');
                _rewardFee = rewardFee;
}

function setBurnFeePercent(uint256 burnFee) external onlyOwner {
        require(burnFee <= 8, 'Tax exceeds maximum 8%');
                _burnFee = burnFee;
}

function setProjectFeePercent(uint256 projectFee) external onlyOwner {
        require(projectFee <= 5, 'Tax exceeds maximum 5%');
                _projectFee = projectFee;
}

function setMarketingFeePercent(uint256 marketingFee) external onlyOwner {
        require(marketingFee <= 5, 'Tax exceeds maximum 5%');
                _marketingFee = marketingFee;
}

function setCharityFeePercent(uint256 charityFee) external onlyOwner {
        require(charityFee <= 2, 'Tax exceeds maximum 2%');
                _charityFee = charityFee;
}
```

Contract owner can change max tx amount

```
function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner {
        require(maxTxPercent >= 2, 'maxTxPercent must be greater than 0.2%');
        _maxTxAmount = _tTotal.mul(maxTxPercent).div(
                10**3
        );
}
```

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:	13%
Sell fees:	13%
Max TX:	500000000000000000000
Max Sell:	N/A

Honeypot Risk

Ownership:	Owned
Blacklist:	Not detected
Modify Max TX:	Detected with threshold
Modify Max Sell:	Not detected
Disable Trading:	Not detected

Rug Pull Risk

Liquidity:	N/A
Holders:	Clean

VESTALLYTOKEN TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (1,000,000,000,000,000.00 Tokens) of VesTallyToken

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

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

Rank	Address	Quantity (Token)	Percentage
1	0x30f5b50555ceaf006aabe095b31a6a2b5823e553	1,000,000,000,000,000	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.