freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

maska.

Maska

$MSK

18/11/2023

TOKEN OVERVIEW

Fees

- Buy fees: 5%
- Sell fees: 5%

Fees privileges

- Can change buy fees up to 10% and sell fees up to 10%

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can’t change max tx amount and / or max wallet amount

Blacklist

- Blacklist function not detected

Other privileges

- Can exclude / include from fees
- Contract owner has to call confirmLpFilled function to enable trade

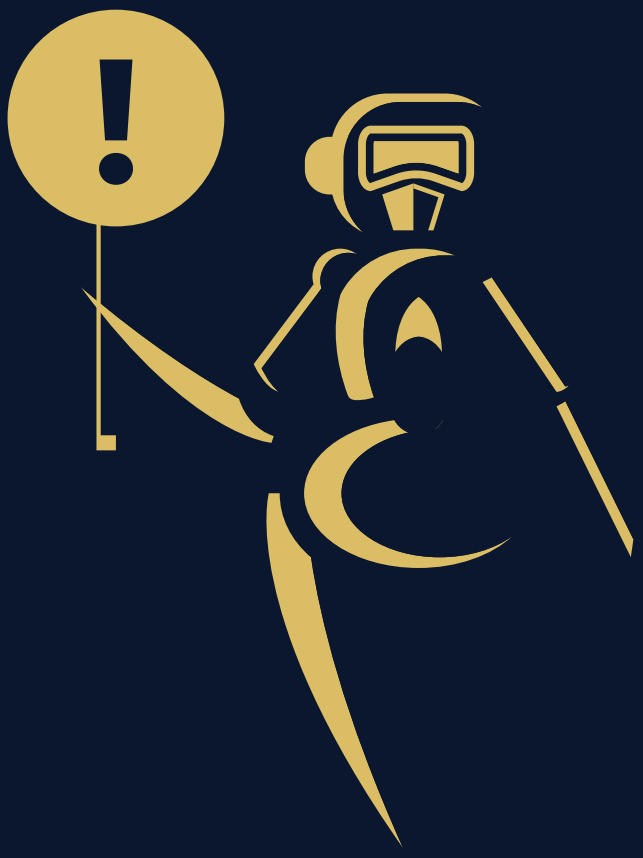
TABLE OF CONTENTS

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

0x2e23d6f6189Ad597f3bBb86a8b822B6B246c2B47

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 18/11/2023

WEBSITE DIAGNOSTIC

https://www.maska.social/

0-49

50-89

90-100

Performance

Accessibility

Best Practices

SEO

Progressive Web App

Socials

Twitter

https://twitter.com/MaskaSocial

Telegram

https://t.me/maska_en

AUDIT OVERVIEW

84

Security Score

98

Static Scan
Automatic scanning for common vulnerabilities

82

ERC Scan
Automatic checks for ERC's conformance

1 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	Low
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 tax

```
function updateExcludedFromFees(address _address, bool state) external onlyOwner {
    excludedFromFees[_address] = state;
}
```

- Contract owner has to call `confirmLpFilled` function to enable trade

Please note that any wallet excluded from fees retains the ability to engage in trading, even in situations where trading has been disabled

```
function confirmLpFilled() external onlyOwner{
    lpFilled = true;
    swapEnabled = true;
}

_transferFrom function line 944
.
.
.
require(lpFilled || excludedFromFees[sender] || excludedFromFees[recipient], "Trading disabled");
.
.
.
```

- Contract owner can change swap settings

```
function setSwapEnabled(bool state) external onlyOwner {
    swapEnabled = state;
}

function setSwapThreshold(uint256 new_amount) external onlyOwner {
    swapThreshold = new_amount * 10**decimals();
}
```

- Contract owner has ability to retrieve any token held by the contract

Native tokens excluded

```
function rescueBEP20(address tokenAddress, uint256 amount) external onlyOwner{
    require(tokenAddress != address(this), "Can't take self token");
    IERC20(tokenAddress).transfer(owner(), amount);
}

function rescueBNB(uint256 weiAmount) external onlyOwner{
    payable(owner()).sendValue(weiAmount);
}
```

Contract owner can change buy fees up to 10% and sell fees up to 10%

```
function setBuyTaxes(uint256 _marketing, uint256 _dev, uint256 _liquidity) external onlyOwner{
        require(
          _marketing + _dev + _liquidity <= 10,
          "Total buy fee is over 10%"
        );
        buyTaxes = Taxes(_marketing, _dev, _liquidity);
        totalBuyTax = _marketing + _dev + _liquidity;
    }

    function setSellTaxes(uint256 _marketing, uint256 _dev, uint256 _liquidity) external onlyOwner{
        require(
          _marketing + _dev + _liquidity <= 10,
          "Total sell fee is over 10%"
        );
        sellTaxes = Taxes(_marketing, _dev, _liquidity);
        totalSellTax = _marketing + _dev + _liquidity;
    }
```

Contract owner can change marketingWallet and devFunds addresses

Current values:

marketingWallet : 0x0000000000000000000000000000000000000000

devFunds : 0x0000000000000000000000000000000000000000

```
function updateMarketingWallet(address newWallet) external onlyOwner{
        require(newWallet != address(0), "Marketing wallet cannot be zero");
        marketingWallet = newWallet;
    }

    function updateDevFunds(address newWallet) external onlyOwner{
        require(newWallet != address(0), "Dev wallet cannot be zero");
        devFunds = newWallet;
    }
```

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
        _transferOwnership(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");
        _transferOwnership(newOwner);
    }

    function _transferOwnership(address newOwner) internal virtual {
        address oldOwner = _owner;
        _owner = newOwner;
        emit OwnershipTransferred(oldOwner, newOwner);
    }
```

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 1 HIGH issues 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:	100% unlocked tokens

MSK TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

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

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

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

Rank	Address	Quantity (Token)	Percentage
1	Socaverse: Deployer	1,000,000,000	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.