freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

MCA

$MCA

15/11/2023

TOKEN OVERVIEW

Fees

- Buy fees: 15%
- Sell fees: 15%

Fees privileges

- Can’t change fees

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 detected

Other privileges

- Can exclude / include from fees
- Contract owner can set isPaused to true and block transfer function (whitelisted wallets excluded)

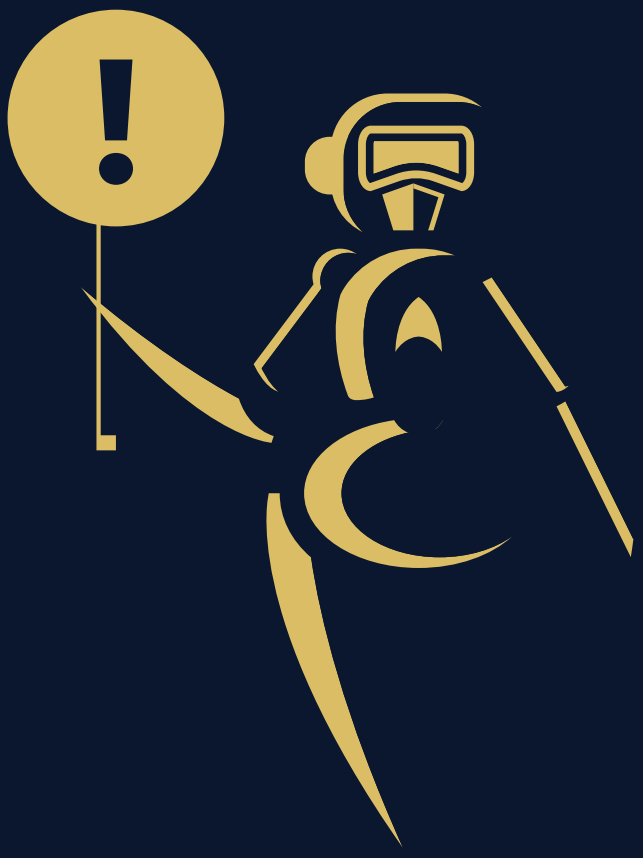
TABLE OF CONTENTS

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

0x666bA0eDfd315861e95F7EAB2Ec91426E5248b32

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 15/11/2023

WEBSITE DIAGNOSTIC

https://meccanft.com/


0-49


50-89


90-100

Performance

Accessibility

Best Practices

SEO

Progressive Web App

Socials


Twitter

https://twitter.com/meccafoundation


Telegram

https://t.me/meccanft

AUDIT OVERVIEW

61

Security Score
HIGH RISK
Audit FAIL

93

Static Scan
Automatic scanning for common vulnerabilities

66

ERC Scan
Automatic checks for ERC's conformance

2	High
0	Medium
0	Low
0	Optimizations
0	Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Low
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 exclude addresses from transactions

  In summary, when isPaused is true, the contract imposes additional restrictions on normal transfers by requiring the recipient to be whitelisted.

```
function onPaused() public onlyAdmin {
      isPaused = true;
}

function offPaused() public onlyAdmin {
      isPaused = false;
}

in _transfer function line 1117
.
.
.
if (isPaused) {
                require(whitelist[to] == true, "100");
}
.
.
.
```

- Contract owner can change poolAddress, admin and addLiquidityAddress addresses

  Current values:

  poolAddress: 0x1CA34FD6a444c58ccdAacF3B7c28F9905A71263c

  admin: 0x933C597d3F992b9C5426b193C4322675E3cB1866

  addLiquidityAddress: 0x2a7a7c01D0ba4F3F7FB128DE8fBA51D1A2AfFcce

```
function setPoolAdddress(address _address) public onlyAdmin {
      whitelist[_address] = true;
      poolAdddress = _address;
}

function setAdmin(address _address) public onlyAdmin {
      admin = _address;
}

function setAddLiquidityAddress(address _address) public onlyAdmin {
      addLiquidityAddress = _address;
}
```

Contract owner can burn tokens

Constants.burnAddress line 10 (File 7 or 11 Constants.sol);

address constant burnAddress = 0x000000000000000000000000000000000000dEaD;

```
function destroy(uint256 amount) public onlyAdmin {
    _transfer(address(this), Constants.burnAddress, amount);
    destroyTotal += amount;
}
```

Constructor arguments:

-----Decoded View----------

Arg [0] : _lq (address): 0x2a7a7c01D0ba4F3F7FB128DE8fBA51D1A2AfFcce

Arg [1] : _feeAddress (address): 0x05897EB79C6B1d1EaB50925AFDb9B6bc10EdA0B1

Arg [2] : _poolAdddress (address): 0x1CA34FD6a444c58ccdAacF3B7c28F9905A71263c

Arg [3] : _destroyAddress (address): 0x14f8DC97218f35782c935D6B9BfD8B3aF33e84EE

_poolAddress is set to 0x1CA34FD6a444c58ccdAacF3B7c28F9905A71263c contract TransparentUpgradeableProxy

The implementation contract at 0x16d8f1137a0efd88f0e91d9e12b5c571c021c1ca does not seem to be verified.

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 2 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	15%
Sell fees:	15%
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

Ownership:	Owned
Blacklist:	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

MCA TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

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

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	0x2a7a7c...A2AfFcce	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.