



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



MeshWave
\$MWAVE

29/03/2024



TOKEN OVERVIEW

Fees

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

Fees privileges

- Can change buy fees up to 95% and sell fees up to 95%

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can change max tx amount and max wallet amount (without threshold)

Blacklist

- Blacklist function not detected

Other privileges

- Can exclude / include from fees
 - Contract owner has the ability to enable / disable trade
-

TABLE OF CONTENTS

1

DISCLAIMER

2

INTRODUCTION

3

WEBSITE + SOCIALS

4-5

AUDIT OVERVIEW

6-8

OWNER PRIVILEGES

9

CONCLUSION AND ANALYSIS

10

TOKEN DETAILS

11

MWAVE ANALYTICS &
TOP 10 TOKEN HOLDERS

12

TECHNICAL DISCLAIMER



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

0x4447743d42680F7fbB56e87b3617463113ca649E

Network: **Ethereum (ETH)**

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on **29/03/2024**



WEBSITE DIAGNOSTIC

<https://meshwave.ai/>



0-49



50-89



90-100



Performance



Accessibility



Best
Practices



SEO



Progressive
Web App

Socials



Twitter

<https://twitter.com/meshwaveai>



Telegram

N/A

AUDIT OVERVIEW



Security Score
HIGH RISK
Audit FAIL



Static Scan
Automatic scanning for
common vulnerabilities



ERC Scan
Automatic checks for
ERC's conformance



High



Medium



Low



Optimizations



Informational



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

- Contract owner can enable / disable trade

```
function switchTrading(bool _marketOpened) public onlyOwner {  
    marketOpened = _marketOpened;  
}
```

- Contract owner can change max tx amount limitation (without threshold)

Note that setting the value too low may prevent users from making purchase transactions

```
function setMaxTxnAmount(uint256 maxTxAmount) public onlyOwner {  
    _maxTxnSize = maxTxAmount;  
}
```

- Contract owner can change max wallet amount limitation (without threshold)

Note that setting the value too low may prevent users from making purchase transactions

```
function setMaxHoldSize(uint256 maxHoldSize) public onlyOwner {  
    _maxHoldSize = maxHoldSize;  
}
```

- Contract owner can change buy fees up to 95% and sell fees up to 95%

```
function updateFee(uint256 feeOnBuy, uint256 feeOnSell) public onlyOwner {  
    require(  
        feeOnBuy >= 0 && feeOnBuy <= 95,  
        "Buy tax must be between 0% and 95%"  
    );  
    require(  
        feeOnSell >= 0 && feeOnSell <= 95,  
        "Sell tax must be between 0% and 95%"  
    );  
    _feeOnBuy = feeOnBuy;  
    _feeOnSell = feeOnSell;  
}
```

● Contract owner can change swap settings (without threshold)

```
function setMinSwapTokensThreshold(uint256 minSwappableAmount)
    public
    onlyOwner
{
    _minSwappableAmount = minSwappableAmount;
}

function toggleautoSwapEnabled(bool _autoSwapEnabled) public onlyOwner {
    autoSwapEnabled = _autoSwapEnabled;
}
```

● Contract owner can exclude / include wallet(s) from tax

```
function excludeMultipleAccountsFromFees(
    address[] calldata accounts,
    bool excluded
) public onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromFee[accounts[i]] = excluded;
    }
}
```

● 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 renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _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 4 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	5%
Sell fees:	5%
Max TX:	1,000,000
Max Wallet:	2,000,000

Honeypot Risk

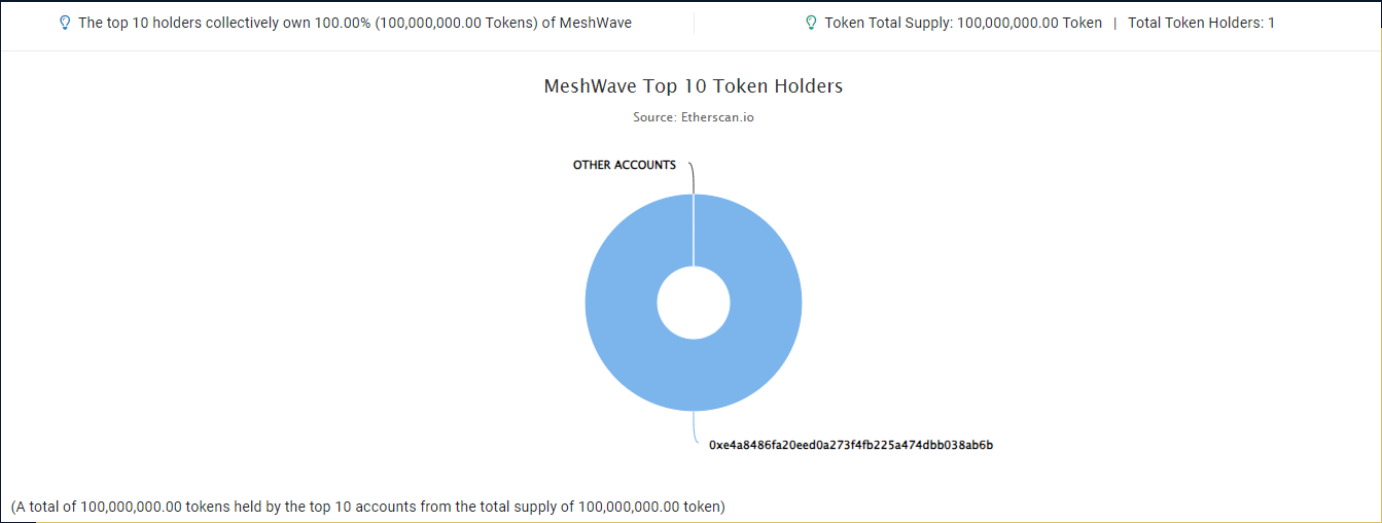
Ownership:	Owned
Blacklist:	Not detected
Modify Max TX:	Detected
Modify Max Sell:	Not detected
Disable Trading:	Detected

Rug Pull Risk

Liquidity:	N/A
Holders:	100% unlocked tokens



MWAVE TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS



Rank	Address	Quantity (Token)	Percentage
1	0xe4A8486f...bb038Ab6B	100,000,000	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.

