



freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Dragoland
\$DRAGO



10/01/2022



TABLE OF CONTENTS

- 1 DISCLAIMER
- 2 INTRODUCTION
- 3-4 WEBSITE DIAGNOSTIC
- 5-6 AUDIT OVERVIEW
- 7 OWNER PRIVILEGES
- 8 CONCLUSION AND ANALYSIS
- 9 TOKEN DETAILS
- 10 DRAGOLAND TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS
- 11 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 Dragoland (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x3D87f8923c3a16c5AB5D460ffA548418b58d9Fd8

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 10/01/2022



WEBSITE DIAGNOSTIC

<https://dragoland.io/>



0-49



50-89



90-100



Performance



Accessability



Best Practices



SEO



Progressive
Web App

Metrics



First Contentful Paint

3.4 s



Time to interactive

5.8 s



Speed Index

14.1 s



Total Blocking Time

0.4 ms



Large Contentful Paint

24.1 s



Cumulative Layout Shift

0.022

Issues found

Use video formats for animated content

Properly size images

Reduce unused JavaScript

Eliminate render-blocking resources

Avoid enormous network payloads - Total size was 23,951 KiB

Ensure text remains visible during webfont load

Image elements do not have explicit width and height

Reduce JavaScript execution time - 8.6 s

AUDIT OVERVIEW



Security Score



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	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 exclude/include from fees a wallet or multiple wallets

```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    require(_isExcludedFromFees[account] != excluded, "Drago: Account is already the value of 'excluded'");
    _isExcludedFromFees[account] = excluded;

    emit ExcludeFromFees(account, excluded);
}

.

.

.

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

    emit ExcludeMultipleAccountsFromFees(accounts, excluded);
}
```

Contract owner can change swap tx limits

```
function setswapTokensAtAmount (uint256 value) external onlyOwner{
    swapTokensAtAmount = value;
}
```

Contract owner can change taxes

```
function setDevelopmentFee(uint256 value) external onlyOwner{
    developmentFee = value;
    totalFees = developmentFee.add(marketingFee);
}

function setMarketingFee(uint256 value) external onlyOwner{
    marketingFee = value;
    totalFees = developmentFee.add(marketingFee);
}
```

Contract owner can change buy and sell transaction limits

```
function setMaxBuyTransaction(uint256 maxTxn) external onlyOwner {
    maxBuyTranscationAmount = maxTxn;
}

function setMaxSellTransaction(uint256 maxTxn) external onlyOwner {
    maxSellTransactionAmount = maxTxn;
}
```

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:	6%
Sell fees:	6%
Max TX:	5000000
Max Sell:	5000000

Honeypot Risk

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

Rug Pull Risk

Liquidity:	N/A
Holders:	Clean



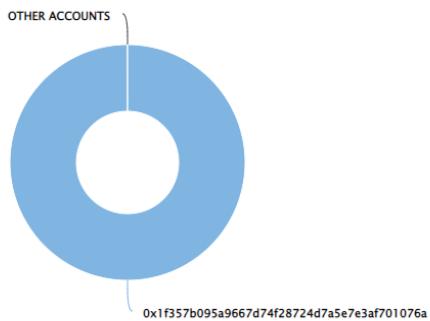
DRAGOLAND TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS

The top 100 holders collectively own 100.00% (1,000,000,000.00 Tokens) of Dragoland

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

Dragoland Top 100 Token Holders

Source: BscScan.com



(A total of 1,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x1f357b095a9667d74f28724d7a5e7e3af701076a	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.

