



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Dragon Wood
\$WOODRA

31/12/2023



TOKEN OVERVIEW

Fees

- Buy fees: 0%
- Sell fees: 0%

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 change max tx amount and max wallet amount (with threshold)

Blacklist

- Blacklist function not detected

Other privileges

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

TABLE OF CONTENTS

1

DISCLAIMER

2

INTRODUCTION

3

WEBSITE + SOCIALS

4-5

AUDIT OVERVIEW

6-9

OWNER PRIVILEGES

10

CONCLUSION AND ANALYSIS

11

TOKEN DETAILS

12

WOODRA TOKEN ANALYTICS &
TOP 10 TOKEN HOLDERS

13

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

0x0DDE4240a425A20F92EBDD2625152A60cf76f2AF

Network: **Ethereum (ETH)**

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on **31/12/2023**



WEBSITE DIAGNOSTIC

Under Development



0-49



50-89



90-100



Performance



Accessibility



Best
Practices



SEO



Progressive
Web App

Socials



Twitter

<https://x.com/DragonWoodETH>



Telegram

<https://t.me/DragonWoodETH>

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'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 excludeFromFees(address account, bool excluded) public onlyOwner {
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}
```

- Contract owner can exclude/include wallet from tx limitations

```
function excludeFromMaxTransaction(address updAds, bool isEx)
    public
    onlyOwner
{
    _isExcludedMaxTransactionAmount[updAds] = isEx;
}
```

- Contract owner has to call **enableTrading** 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 enableTrading() external onlyOwner {
    tradingActive = true;
    swapEnabled = true;
}

_transferFrom function line 1253
.
.
.
if (!tradingActive) {
    require(
        _isExcludedFromFees[from] || _isExcludedFromFees[to],
        "Trading is not active."
    );
}
.
.
.
```

● Contract owner can change swap settings

```
function updateSwapTokensAtAmount(uint256 newAmount)
    external
    onlyOwner
    returns (bool)
{
    require(
        newAmount >= (totalSupply() * 1) / 100000,
        "Swap amount cannot be lower than 0.001% total supply."
    );
    require(
        newAmount <= (totalSupply() * 5) / 1000,
        "Swap amount cannot be higher than 0.5% total supply."
    );
    swapTokensAtAmount = newAmount;
    return true;
}

function updateSwapEnabled(bool enabled) external onlyOwner {
    swapEnabled = enabled;
}
```

● Contract owner can enable/disable limitations

```
function removeLimits() external onlyOwner returns (bool) {
    limitsInEffect = false;
    return true;
}
```

● Contract owner can change tx limitations and wallet limitations (with threshold)

```
function updateMaxTxnAmount(uint256 newNum) external onlyOwner {
    require(
        newNum >= ((totalSupply() * 5) / 1000) / 1e18,
        "Cannot set maxTransactionAmount lower than 0.5%"
    );
    maxTransactionAmount = newNum ;
    maxWallet = newNum ;
}

function updateMaxWalletAmount(uint256 newNum) external onlyOwner {
    require(
        newNum >= ((totalSupply() * 5) / 1000) / 1e18,
        "Cannot set maxWallet lower than 0.5%"
    );
    maxWallet = newNum ;
}
```

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

```
function updateBuyFees(
    uint256 _LpFee,
    uint256 _marketingFee,
    uint256 _liquidityFee,
    uint256 _devFee
) external onlyOwner {
    require((_LpFee + _marketingFee + _liquidityFee + _devFee) <= 10, "Max BuyFee 10%");
    buyLpFee = _LpFee;
    buyMarketingFee = _marketingFee;
    buyLiquidityFee = _liquidityFee;
    buyDevFee = _devFee;
    buyTotalFees = buyLpFee + buyMarketingFee + buyLiquidityFee + buyDevFee;
}

function updateSellFees(
    uint256 _LpFee,
    uint256 _marketingFee,
    uint256 _liquidityFee,
    uint256 _devFee
) external onlyOwner {
    require((_LpFee + _marketingFee + _liquidityFee + _devFee) <= 10, "Max SellFee 10%");
    sellLpFee = _LpFee;
    sellMarketingFee = _marketingFee;
    sellLiquidityFee = _liquidityFee;
    sellDevFee = _devFee;
    sellTotalFees = sellLpFee + sellMarketingFee + sellLiquidityFee + sellDevFee;
}
```

● Contract owner can turn off the transfer delay feature

If the transfer delay is enabled, it restricts purchases to one per block. The block time in Ethereum is designed to be approximately 15 seconds

```
function disableTransferDelay() external onlyOwner returns (bool) {
    transferDelayEnabled = false;
    return true;
}
```

● Contract owner can transfer ownership

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

● Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
    _transferOwnership(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 1 HIGH issues during the first review.

TOKEN DETAILS

Details

| | |
|------------|-----------------|
| Buy fees: | 0% |
| Sell fees: | 0% |
| Max TX: | 429,000,000,000 |
| Max Sell: | 429,000,000,000 |

Honeypot Risk

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

Rug Pull Risk

| | |
|------------|----------------------|
| Liquidity: | N/A |
| Holders: | 100% unlocked tokens |



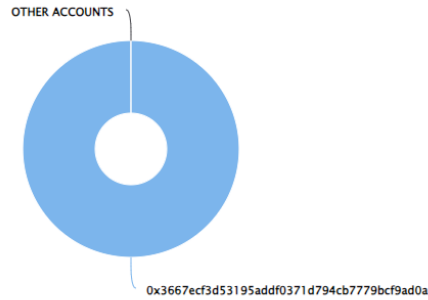
WOODRA TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (429,000,000,000.00 Tokens) of Dragon Wood


Token Total Supply: 429,000,000,000.00 Token | Total Token Holders: 1

Dragon Wood Top 10 Token Holders

Source: Etherscan.io



(A total of 429,000,000,000.00 tokens held by the top 10 accounts from the total supply of 429,000,000,000.00 token)

| Rank | Address | Quantity (Token) | Percentage |
|------|---|------------------|------------|
| 1 | 0x3667Ec...bcf9ad0a  | 429,000,000,000 | 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.

