



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



House of the Dragon
\$HOTD

31/07/2022



TABLE OF CONTENTS

- 1 **DISCLAIMER**
- 2 **INTRODUCTION**
- 3-4 **AUDIT OVERVIEW**
- 5-6 **OWNER PRIVILEGES**
- 7 **CONCLUSION AND ANALYSIS**
- 8 **TOKEN DETAILS**
- 9 **HOUSE OF THE DRAGON TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS**
- 10 **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 Honey pot etc)



INTRODUCTION

FreshCoins (Consultant) was contracted by **House of the Dragon** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x37eD5832B718FF2D327d78A5eaF1c5315669f97f

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 **31/07/2022**



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	Passed
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 change swap status

```
function setSwapReservesEnabled(bool isEnabled_) external onlyOwner {
    swapReserves = isEnabled_;
}
```

- Contract owner can exclude/include wallet from tax

```
function setExcludedFromTax(address wallet_, bool isExcluded_)
    external
    onlyOwner
{
    excludedFromTax[wallet_] = isExcluded_;
}
```

- Contract owner can change marketingWallet address

```
function setMarketingWallet(address newMarketingWallet_)
    external
    onlyOwner
{
    require(
        newMarketingWallet_ != marketingWallet,
        "ReflectionERC20: same as current wallet"
    );
    require(
        newMarketingWallet_ != address(0),
        "ReflectionERC20: cannot be address(0)"
    );
    marketingWallet = newMarketingWallet_;
    excludedFromTax[newMarketingWallet_];
}
```

- Contract owner can enable/disable tax

```
function setTaxEnabled(bool isEnabled_) external onlyOwner {
    if (reserves > 0) processReserves();
    taxEnabled = isEnabled_;
}
```

● 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 0 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees: 6%

Sell fees: 6%

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: Clean



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.

