SMART CONTRACT SECURITY AUDIT

WATCHTOWER

DISCLAIMER

Watchtower has completed this report to provide a summary of the Smart Contract functions, and any security, dependency or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as at the date of this report. In order to understand the full scope of our analysis, it is vital for you to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against Watchtower or it's Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your own independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

DISCLAIMER: By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any and all duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise, and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and Watchtower and its members (including holding companies, shareholders, backups, representatives, chiefs, officers and other agents) Watchtower and it's subsidiaries owe no obligation of care towards you or any other person, nor does Watchtower make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:
Watchtower is an Anti-Scam Token Utility which reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity.
Watchtowers Development Team consists of a number of Smart Contract creators, Auditors Developers and Blockchain experts.
Watchtowers Website Scanner reviews a number of Risk factors to provide an adequate Risk summary of token projects.
In Addition to this the team also helps with Creation of Smart Contracts for legitimate projects, Audits and Promotion.

OVERVIEW

Watchtower was commissioned by DragonBall Inu to complete a Smart Contract audit.
The objective of the Audit is to achieve the following:

- Review the Project and experience and Development team
- Ensure that the Smart Contract functions are necessary and operate as intended.
- Identify any vulnerabilities in the Smart Contract code.

DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or provide financial advice in any way, All investments are made at your own risk.
(https://www.cryptowatchtower.io/)

SMART CONTRACT REVIEW

Contract Created on the 9th November 2021 **Solidity compiler v0.8.9**

Contract name	DragonBall Inu
Contract address	0xAf0265a64077b9B3912878DFbDdf71D22144bc37
Total supply	100,000,000,000,000
Token ticker	DBI
Decimals	9
Token holders	4
Transactions count	4
Top 5 holders dominance	NOT LAUNCHED
Tax fee	9%
Total fees	9% ~ BUY / 15% ~ SELL
Contract deployer address	0x5fb71Dbf7248a01bf96cE2AB2DA34EEAbE58c261
Contract's current owner address	0x1F8a2745740DbfC006a2e4448c7016ffa00D3570

Project Overview

Project Details: (Website: https://dragonballinu.io/)

Dragonball Inu team is building a Swap with low fees and a rewards ecosystem that focuses on security for holders with minimal impermanent losses when staking.
The team is also developing an NFT Marketplace and DragonBall Inu NFTs'. More details can be found on the website.

Tokenomics:

Starting Supply: 100,000,000,000,000 (100 Trillion)
9% Tax for Buys and 15% for Sells comprising of:

BUY/SELL

BUY: 5% BNB Rewards / SELL: 7% BNB Rewards
BUY: 2% Liquidity / SELL: 4% Liquidity
BUY: 2% Marketing / SELL: 4% Marketing

Team Review:

Watchtower reviewed a number of factors including the teams background and Cryptocurrency experience, social media interaction and availability, project momentum, token risks and community trust score.
The DragonBall Inu team have a good levels of Cryptocurrency and development knowledge. They are building multiple utilities including a staking pool, NFT Marketplace and NFT's.
The Social score could be better as they only have 1763 followers on telegram and approximately 1261 on Twitter at the time of audit.
In order to maintain buy pressure with a rewards token the team will need to increase their following.

TEAM DOXXED:

We are not aware of the the team being doxxed and the team has not been doxxed to Watchtower.

CONTRACT FUNCTIONS DETAILS

Functions (Public)

This contract has 24 available public functions which the owner can call.
These functions were identified to be safe and can be viewed on BSC Scan or through a DAPP.

LINK:

https://bscscan.com/token/0xaf0265a64077b9b3912878dfbddf71d22144bc37#writeContract

Function risks:

-No Scam Functions Identified!

Imported Libraries / Interfaces

- Context
- Ownable
- IERC20
- IERC20 Metadata
- DividendPayingTokenOptionalInterface
- DividendPayingTokenInterface
- SafeMathInt
- SafeMathUint
- SafeMath
- ERC20
- DividendPayingToken (https://github.com/roger-wu) + edits
- IUniswapV2Router01
- IUniswapV2Router02
- IUniswapV2Factory
- IUniswapV2Pair

Overview

1. ADDITION OF COMMENTS: 10
2. CALL STACK DEPTH ATTACK: 10
3. TIME STAMP DEPENDENCY: 10
4. PARTY MULTISIG BUG: 10
5. USE OF LIBRARIES/DEPENDENCIES (FROM TRUSTED SOURCES): 10
    a. TRANSACTION-ORDERING DEPENDENCY: 10
6. ACCESS CONTROL AND AUTHORIZATION: 10
7. REENTRANCY ATTACKS: 10
8. ERC/BEP STANDARD VIOLATIONS: 10
9. USAGE OF VISIBILITY LEVELS: 10

ISSUES CHECKING STATUS

Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Passed
10. Methods execution permissions.	Passed

Issue description	Checking status
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed

SECURITY ISSUES

High Severity Issues

Nil

Medium Severity Issues

UpdateDividendMinimum() can be bypassed:

- If the owner decides to increase the minimumTokenBalanceForDividends the users must make a transaction to trigger setBalance() and let the contract check if the new limit is respected. So, if a user doesn't move his tokens after the function is called, and his balance is lower than minimum amount, he can still receive rewards. A possible fix is to add a function that update the balance and call it before the rewards are distributed to that user:

```
function fixBalance(address account, uint256 newBalance) public onlyOwner{
        if(excludedFromDividends[account]) {
        return;
      }

      _setBalance(account, newBalance);
     tokenHoldersMap.set(account, newBalance);
 }
...
...
function processAccount(address account, bool automatic) public onlyOwner returns
        fixBalance(account, balanceOf(account));
        uint256 amount = _withdrawDividendOfUser(account);

      if(amount > 0) {
        lastClaimTimes[account] = block.timestamp;
            emit Claim(account, amount, automatic);
        return true;
      }

      return false;
    }
```

SECURITY ISSUES

Medium Severity Issues

IncludeInDividends() doesn't update user dividend balance:
It should be:

```
function includeInDividends(address account) external onlyOwner {
        require(excludedFromDividends[account]);
        excludedFromDividends[account] = false;
        _setBalance(account, balanceOf(account));
        tokenHoldersMap.set(account, balanceOf(account));

        emit IncludeInDividends(account);
    }
```

Low Severity Issues

Lines: 1828- 1838: liquidity, operations and buyback wallets are excluded from fees, so these lines can be removed. Lines 1834-35 already includes them

CONCLUSION

Watchtower reviewed DragonBall Inus' deployed and verified contract to conduct this audit.
Watchtower is satisfied that the contract has no malicious coding and that no severe issues have been found.
The team is using Pinksale Finance to launch their token and pre-sale. Pinksale have been verified to focus on Safe launches with Anti-sniper functions and token distribution criteria.

Watchtower Disclaimer:

Please check the disclaimer page and note, this Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please do your own research. By reading this report you accept and agree to the disclaimer and understand investments are made at your own risk.
(https://www.cryptowatchtower.io/)

Contact Us

@Watchtower_WTW

Watchtower-WTW

Watchtowercrypto