Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

July, 2021

Audit Details

Audited project

CumBlast

Deployer address

0xaA2e3397c80b6f78dCcc921001572F15186CC723

Client contacts:

CumBlast team

Blockchain

Binance Smart Chain

Project website:

Not provided by CumBlast team

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by CumBlast to perform an audit of smart contracts:

https://bscscan.com/address/0xef80cd56dd7b09b923f4058068682ccffc5b58a7#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

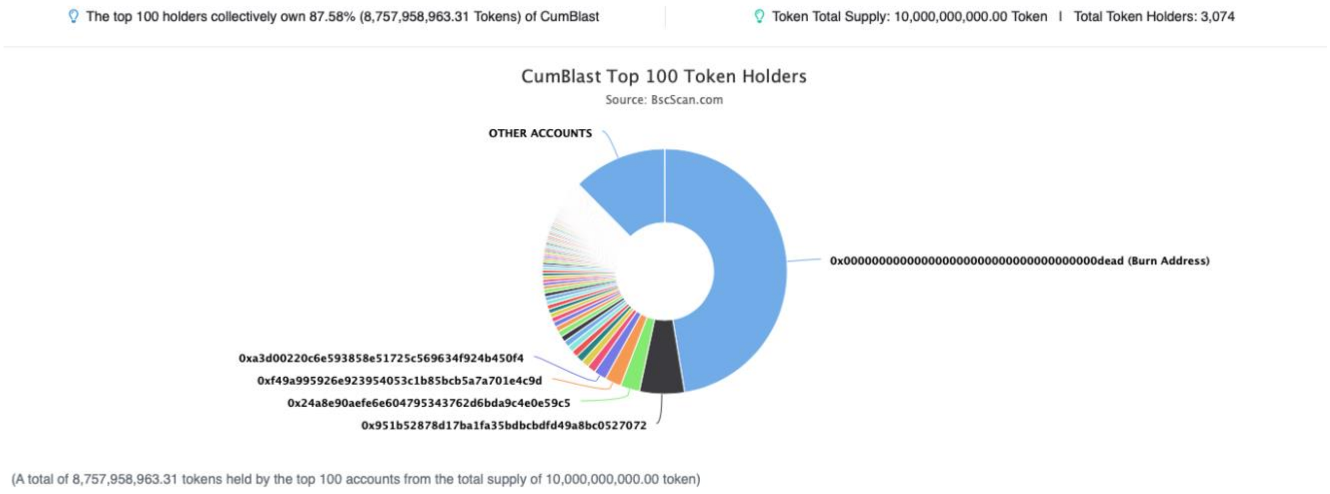
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 13.07.2021

Contract name	CumBlast
Contract address	0xEF80cd56Dd7b09b923F4058068682CCFfc5B58A7
Total supply	10,000,000,000
Token ticker	CBST
Decimals	9
Token holders	3,074
Transactions count	9,398
Top 100 holders dominance	87.58%
Buy/Sell Liquidity fee	5
Buy/Sell reflect fee	2
Buy/Sell marketing fee	3
Total fees	55280087412933380
Uniswap V2 pair	0x10ed43c718714eb63d5aa57b78b54704e256024e
Contract deployer address	0xaA2e3397c80b6f78dCcc921001572F15186CC723
Contract's current owner address	0xaa2e3397c80b6f78dccc921001572f15186cc723

CumBlast Token Distribution



The top 100 holders collectively own 87.58% (8,757,958,963.31 Tokens) of CumBlast

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 3,074

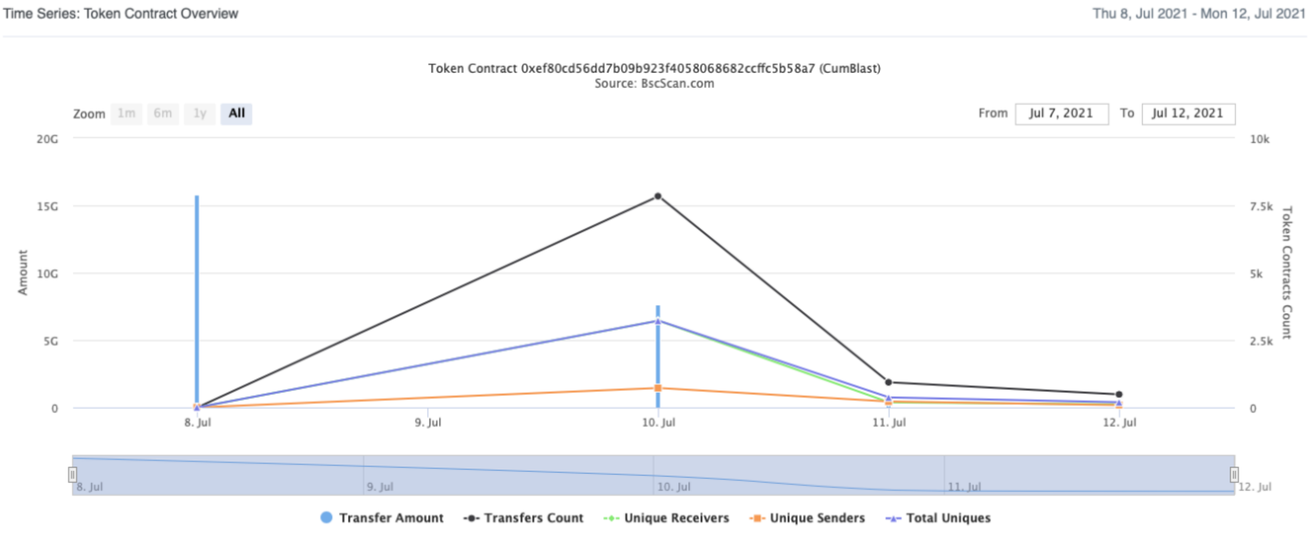
CumBlast Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x000000000000000000000000000000000000dead (Burn Address)
0xa3d00220c6e593858e51725c569634f924b450f4
0xf49a995926e923954053c1b85bcb5a7a701e4c9d
0x24a8e90aefe6e604795343762d6bda9c4e0e59c5
0x951b52878d17ba1fa35bdbcbdfd49a8bc0527072

(A total of 8,757,958,963.31 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

CumBlast Contract Interaction Details



Time Series: Token Contract Overview

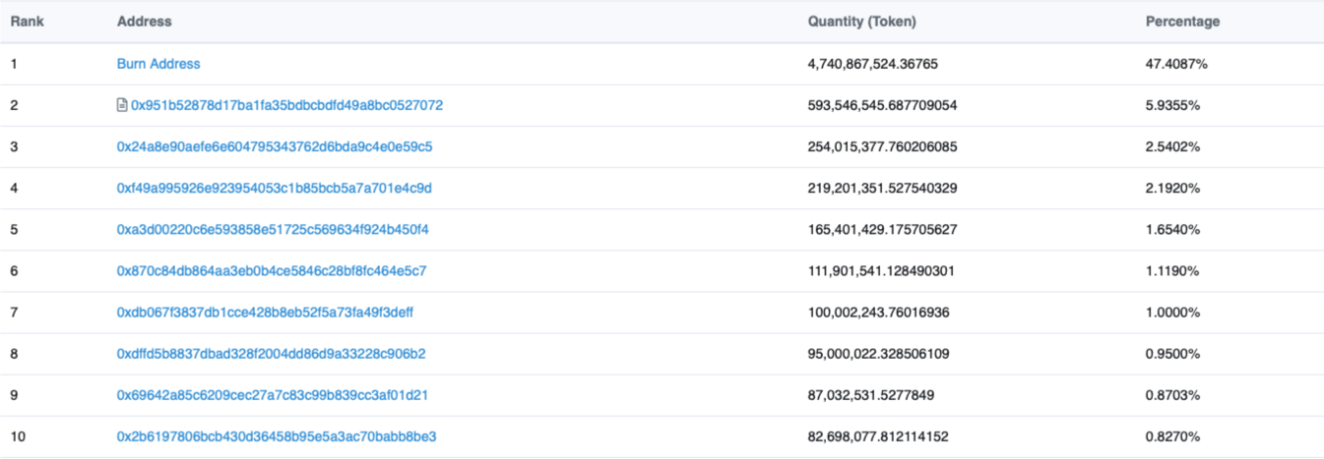
Thu 8, Jul 2021 - Mon 12, Jul 2021

Token Contract 0xef80cd56dd7b09b923f4058068682ccffc5b58a7 (CumBlast)

Source: BscScan.com

From Jul 7, 2021 To Jul 12, 2021

CumBlast Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	Burn Address	4,740,867,524.36765	47.4087%
2	0x951b52878d17ba1fa35bdbcbdfd49a8bc0527072	593,546,545.687709054	5.9355%
3	0x24a8e90aefe6e604795343762d6bda9c4e0e59c5	254,015,377.760206085	2.5402%
4	0xf49a995926e923954053c1b85bcb5a7a701e4c9d	219,201,351.527540329	2.1920%
5	0xa3d00220c6e593858e51725c569634f924b450f4	165,401,429.175705627	1.6540%
6	0x870c84db864aa3eb0b4ce5846c28bf8fc464e5c7	111,901,541.128490301	1.1190%
7	0xdb067f3837db1cce428b8eb52f5a73fa49f3deff	100,002,243.76016936	1.0000%
8	0xdffd5b8837dbad328f2004dd86d9a33228c906b2	95,000,022.328506109	0.9500%
9	0x69642a85c6209cec27a7c83c99b839cc3af01d21	87,032,531.5277849	0.8703%
10	0x2b6197806bcb430d36458b95e5a3ac70babb8be3	82,698,077.812114152	0.8270%

Contract functions details

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setReflectTo #
  - [Ext] setReflectToSetter #

+ [Int] IUniswapV2Pair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #

  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

```
+ CumBlast (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] setRouterAddress #
    - modifiers: onlyOwner
  - [Prv] _hasLimits
  - [Pub] isExcludedFromReward
  - [Pub] isSniperOrBlacklisted
  - [Ext] setBlacklist #
    - modifiers: onlyOwner
  - [Ext] setSniperProtectionEnabled #
    - modifiers: onlyOwner
  - [Ext] setBuyTaxes #
    - modifiers: onlyOwner
  - [Ext] setSellTaxes #
    - modifiers: onlyOwner
  - [Ext] setTransferTaxes #
    - modifiers: onlyOwner
  - [Ext] setRatios #
    - modifiers: onlyOwner
  - [Ext] setMaxTxPercent #
    - modifiers: onlyOwner
  - [Ext] setMarketingWallet #
    - modifiers: onlyOwner
  - [Pub] setSwapAndLiquifyEnabled #
    - modifiers: onlyOwner
  - [Ext] setNewLPHolderToBurn #
    - modifiers: onlyOwner
  - [Ext] excludePresaleAddresses #
    - modifiers: onlyOwner
  - [Pub] excludeFromFee #
    - modifiers: onlyOwner
  - [Ext] includeInFee #
    - modifiers: onlyOwner
  - [Pub] totalFees
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner
  - [Ext] <Fallback> ($)
  - [Prv] _takeReflect #
  - [Prv] _getValues
```

- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] _takeMarketing #
- [Prv] calculateReflectFee
- [Prv] calculateLiquidityFee
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Int] transferToMarketing #
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _checkLiquidityAdd #
- [Prv] _tokenTransfer #
- [Int] adjustTaxes #
- [Prv] _finalizeTransfer #
- [Ext] _busdSwitch #
  - modifiers: onlyOwner

($) = payable function
# = non-constant function

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.	Low issues
10.	Methods execution permissions.	Passed
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

No high severity issues found.

Medium Severity Issues

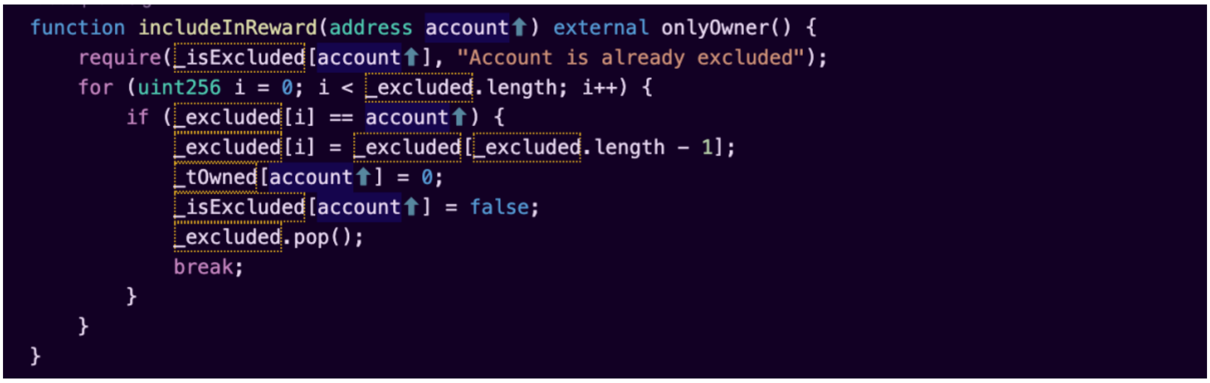
No medium severity issues found.

Low Severity Issues

1. Out of gas

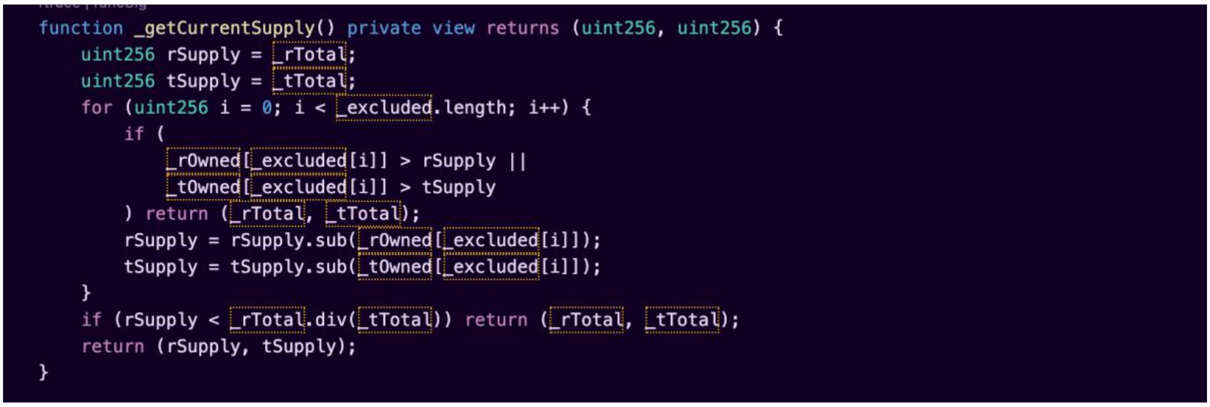
Issue:

- The function includeInReward() uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.



```
function includeInReward(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The function _getCurrentSupply also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.



```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

Notes:

- Marketing fee is taking from transfers to marketing addresses. And taking from liquidity part in swap and liquify.

Owner privileges (In the period when the owner is not renounced)

- Owner can change router address.
- Owner can blacklist addresses.
- Owner can enable and disable sniper protection.
- Owner can change buy/sell/transfer taxes.
- Owner can change marketing and liquidity ratio.
- Owner can change the maximum transaction amount.
- Owner can change marketing wallet address.
- Owner can enable and disable swap and liquify.
- Owner can change liquidity receiver address.
- Owner can exclude addresses from fee, reward and add to _liquidityHolders storage and presaleAddresses storage.
- Owner can exclude from the fee.
- Owner can disable and enable BUSD marketing transfer.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:
https://dxsale.app/app/v2_9/defipresale?saleID=683&chain=BSC

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.