TechRate

Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	MoonBreaker Token
Deployer address:	0xa531a207a991f2aa2ae305e3a0332fb1561ccba6
Client contacts:	MoonBreaker Token team
Blockchain:	Binance Smart Chain
Project website:	https://moonbreakertoken.com

May, 2021
TechRate

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 MoonBreaker Token to perform an audit of smart contracts:

- *https://bscscan.com/address/0x8656093690a2ee6fa80a85e546bf02b81408119a#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.

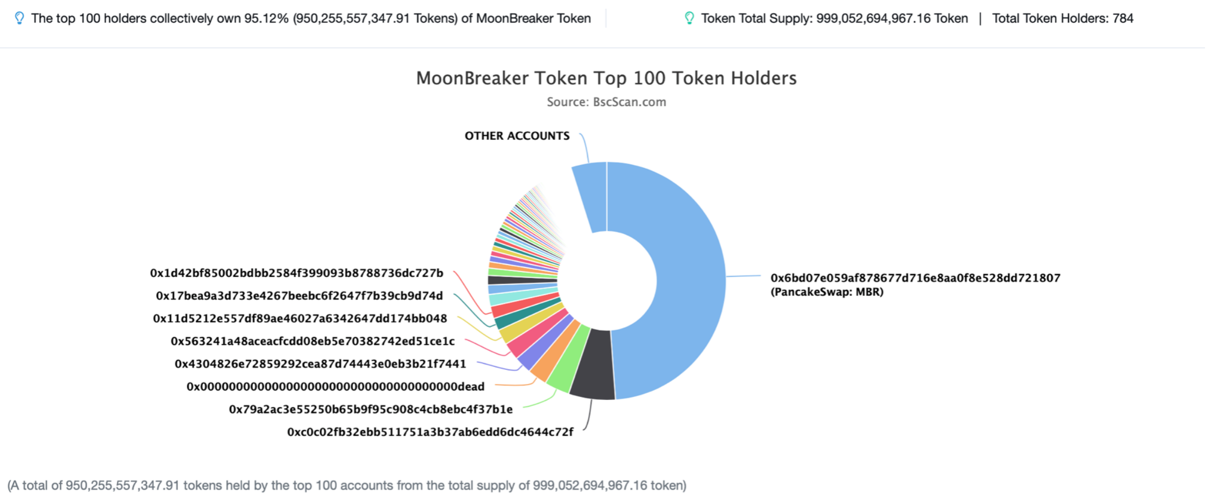
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 02.05.2021.

Contract name:	MoonBreaker Token
Contract address:	0x8656093690a2ee6fa80a85e546bf02b81408119a
Total supply:	999_052_932_129_776_009_169_236_300_503
Token ticker:	MBR
Decimals:	18
Token holders:	784
Transactions count:	2532
Top 100 holders dominance:	95.12 %
Dev fee:	1
Tax fee:	5
Burn fee:	4
Total burn:	947_067_870_223_990_830_763_699_497
Total dev BNB:	118_383_564_207_823_935_945_187_436
Total fees:	118_383_564_207_823_935_945_187_436
Uniswap V2 pair:	0x6bd07e059af878677d716e8aa0f8e528dd721807
Contract deployer address:	0xa531a207a991f2aa2ae305e3a0332fb1561ccba6
Contract’s current owner address:	0x0000000000000000000000000000000000000000

MoonBreaker Token token distribution



The top 100 holders collectively own 95.12% (950,255,557,347.91 Tokens) of MoonBreaker Token

Token Total Supply: 999,052,694,967.16 Token | Total Token Holders: 784

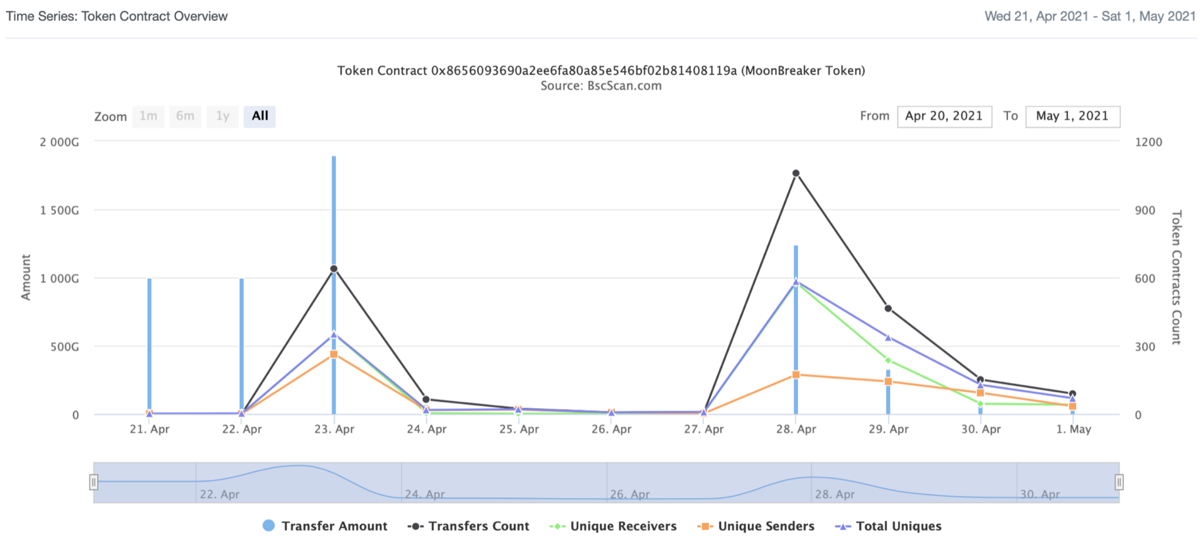
MoonBreaker Token Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x6bd07e059af878677d716e8aa0f8e528dd721807
(PancakeSwap: MBR)
0x1d42bf85002bdbb2584f399093b8788736dc727b
0x17bea9a3d733e4267beebc6f2647f7b39cb9d74d
0x11d5212e557df89ae46027a6342647dd174bb048
0x563241a48aceacfcdd08eb5e70382742ed51ce1c
0x4304826e72859292cea87d74443e0eb3b21f7441
0x000000000000000000000000000000000000dead
0x79a2ac3e55250b65b9f95c908c4cb8ebc4f37b1e
0xc0c02fb32ebb511751a3b37ab6edd6dc4644c72f

(A total of 950,255,557,347.91 tokens held by the top 100 accounts from the total supply of 999,052,694,967.16 token)

MoonBreaker Token contract interaction details



Time Series: Token Contract Overview

Wed 21, Apr 2021 - Sat 1, May 2021

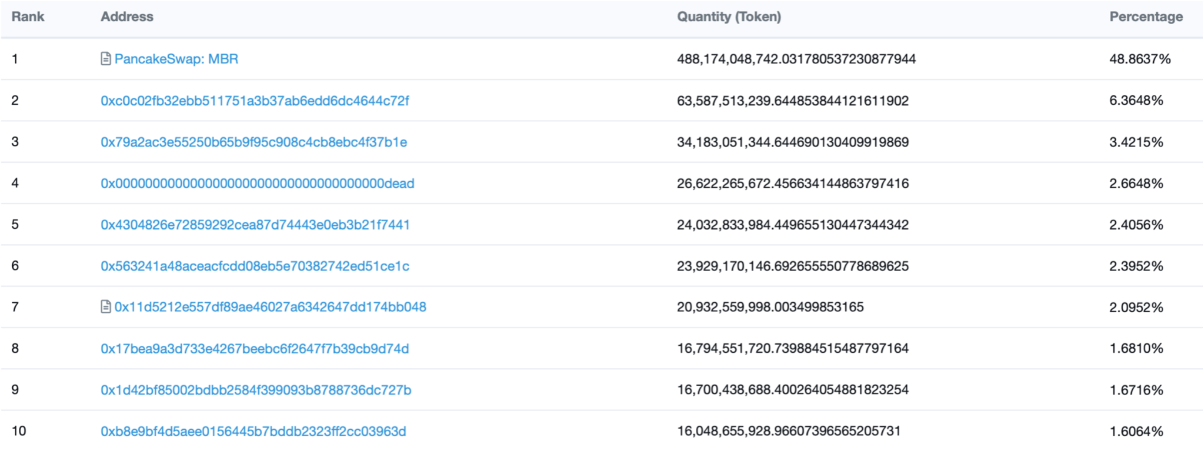
Token Contract 0x8656093690a2ee6fa80a85e546bf02b81408119a (MoonBreaker Token)

Source: BscScan.com

Zoom: 1m 6m 1y All

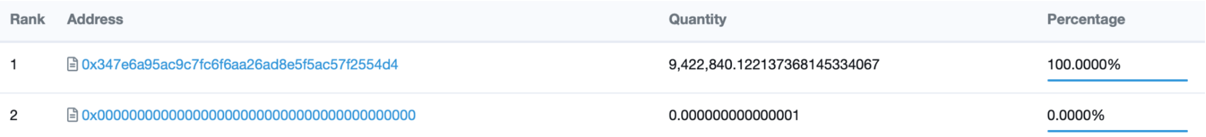
From: Apr 20, 2021 To: May 1, 2021

MoonBreaker Token top 10 token holders



Rank	Address	Quantity (Token)	Percentage
1	📄 PancakeSwap: MBR	488,174,048,742.031780537230877944	48.8637%
2	0xc0c02fb32ebb511751a3b37ab6edd6dc4644c72f	63,587,513,239.644853844121611902	6.3648%
3	0x79a2ac3e55250b65b9f95c908c4cb8ebc4f37b1e	34,183,051,344.644690130409919869	3.4215%
4	0x000000000000000000000000000000000000dead	26,622,265,672.456634144863797416	2.6648%
5	0x4304826e72859292cea87d74443e0eb3b21f7441	24,032,833,984.449655130447344342	2.4056%
6	0x563241a48aceacfcdd08eb5e70382742ed51ce1c	23,929,170,146.692655550778689625	2.3952%
7	📄 0x11d5212e557df89ae46027a6342647dd174bb048	20,932,559,998.003499853165	2.0952%
8	0x17bea9a3d733e4267beebc6f2647f7b39cb9d74d	16,794,551,720.739884515487797164	1.6810%
9	0x1d42bf85002bdbb2584f399093b8788736dc727b	16,700,438,688.400264054881823254	1.6716%
10	0xb8e9bf4d5aee0156445b7bddb2323ff2cc03963d	16,048,655,928.966073965652057 31	1.6064%

MoonBreaker Token LP token holders



Rank	Address	Quantity	Percentage
1	📄 0x347e6a95ac9c7fc6f6aa26ad8e5f5ac57f2554d4	9,422,840.122137368145334067	100.0000%
2	📄 0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%

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 #

+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] getUnlockTime
  - [Pub] getTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #

```
+ [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [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] 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 #

+  MoonBreakerToken (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] isExcludedFromReward
  - [Pub] totalFees
  - [Pub] totalBurn
  - [Pub] totalDevBNB
  - [Pub] minimumTokensBeforeSwapAmount
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner
  - [Prv] _approve #
  - [Prv] _transfer #
  - [Prv] swapAndLiquify #
```

    - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateBurnFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Pub] excludeFromFee #
    - modifiers: onlyOwner
- [Pub] includeInFee #
    - modifiers: onlyOwner
- [Ext] setTaxFeePercent #
    - modifiers: onlyOwner
- [Ext] setBurnFeePercent #
    - modifiers: onlyOwner
- [Ext] setDevFeePercent #
    - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
    - modifiers: onlyOwner
- [Ext] setNumTokensSellToAddToLiquidity #
    - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
    - modifiers: onlyOwner
- [Prv] TransferDevETH #
- [Ext] <Fallback> ($)

($) = 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

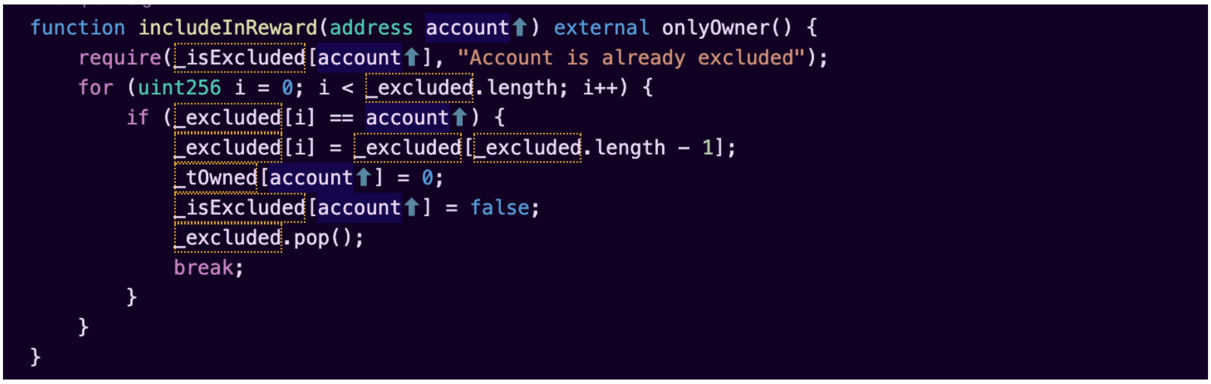
No medium severity issues found.

Low Severity Issues

1. Out of gas

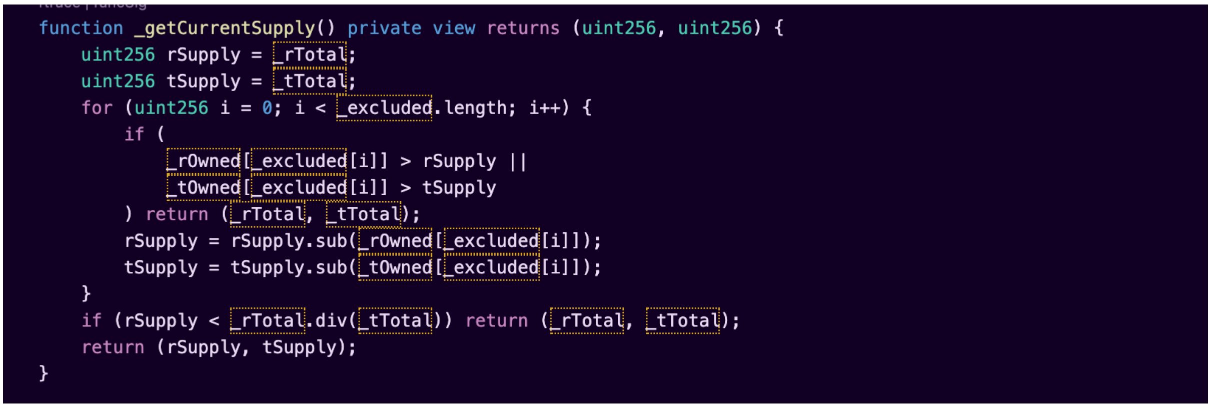
Issue:

- 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:

Use EnumerableSet instead of array or do not use long arrays.

Conclusion

Smart contracts contain low severity issues! No liquidity info found on DXSale or Unicrypt, liquidity pair contract is not checked.

In swapAndLiquify function balance of the contract will be sent to the dev address.

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.