TechRate

Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	CryptoNaught
Deployer address:	0x7985320701eddbbe2a5887e8ca198aed88997a70
Client contacts:	CryptoNaught team
Blockchain:	Binance Smart Chain
Project website:	https://cryptonaughts.finance

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 CryptoNaught to perform an audit of smart contracts:

- *https://bscscan.com/address/0x1ad7dbe0d521ca1ae72decc06f1570aa43c781a2#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.

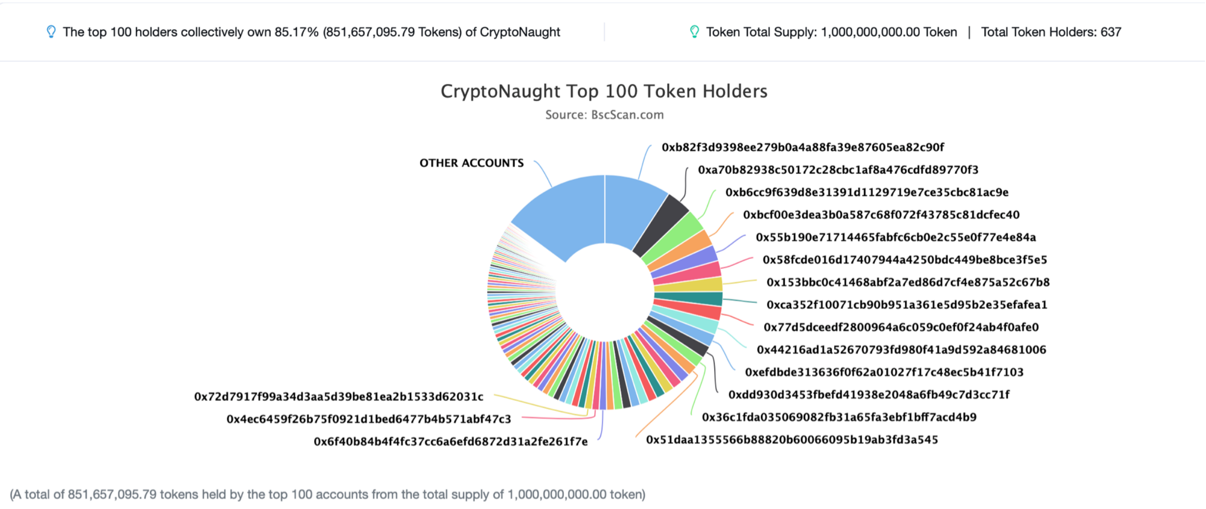
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 07.05.2021.

Contract name:	CryptoNaught
Contract address:	0x1ad7dbe0d521ca1ae72decc06f1570aa43c781a2
Total supply:	1000000000000000000000000000
Token ticker:	CRYPT
Decimals:	18
Token holders:	637
Transactions count:	1825
Top 100 holders dominance:	85.17 %
Liquidity fee:	5
Tax fee:	1
Total fees:	20812731963249040051570620
Uniswap V2 pair:	0xb82f3d9398ee279b0a4a88fa39e87605ea82c90f
Contract deployer address:	0x7985320701eddbbe2a5887e8ca198aed88997a70
Contract’s current owner address:	0xdc3745944b6b619b2ee48f1fd35556bf7d86e0c6

CryptoNaught token distribution



The top 100 holders collectively own 85.17% (851,657,095.79 Tokens) of CryptoNaught

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 637

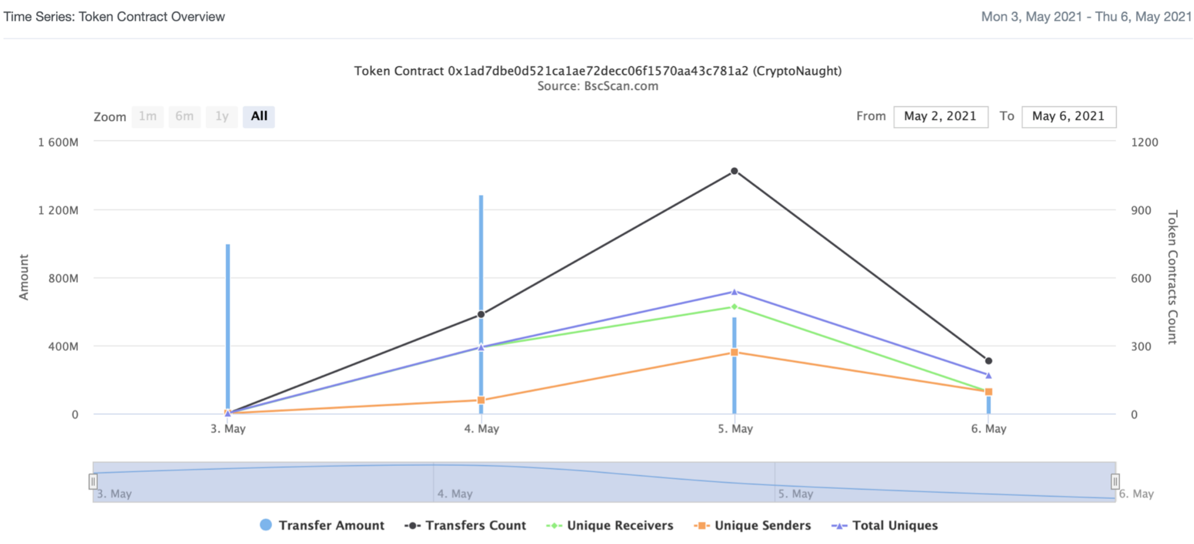
CryptoNaught Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xb82f3d9398ee279b0a4a88fa39e87605ea82c90f
0xa70b82938c50172c28cbc1af8a476cdfd89770f3
0xb6cc9f639d8e31391d1129719e7ce35cbc81ac9e
0xbcf00e3dea3b0a587c68f072f43785c81dcfec40
0x55b190e71714465fabfc6cb0e2c55e0f77e4e84a
0x58fcde016d17407944a4250bdc449be8bce3f5e5
0x153bbc0c41468abf2a7ed86d7cf4e875a52c67b8
0xca352f10071cb90b951a361e5d95b2e35efafea1
0x77d5dceedf2800964a6c059c0ef0f24ab4f0afe0
0x44216ad1a52670793fd980f41a9d592a84681006
0xefdbde313636f0f62a01027f17c48ec5b41f7103
0xdd930d3453fbefd41938e2048a6fb49c7d3cc71f
0x36c1fda035069082fb31a65fa3ebf1bff7acd4b9
0x51daa1355566b88820b60066095b19ab3fd3a545
0x6f40b84b4f4fc37cc6a6efd6872d31a2fe261f7e
0x4ec6459f26b75f0921d1bed6477b4b571abf47c3
0x72d7917f99a34d3aa5d39be81ea2b1533d62031c

(A total of 851,657,095.79 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

CryptoNaught contract interaction details



Time Series: Token Contract Overview

Mon 3, May 2021 - Thu 6, May 2021

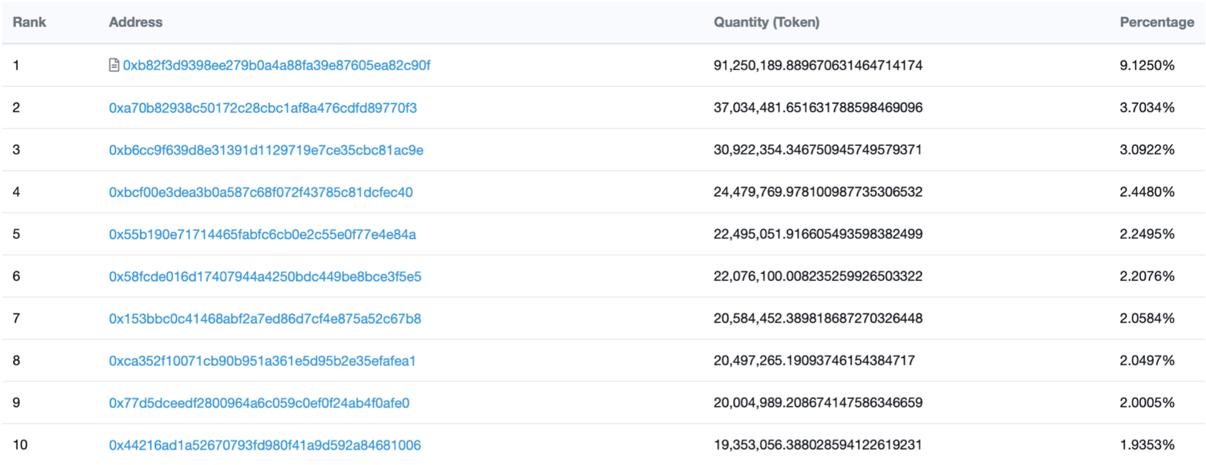
Token Contract 0x1ad7dbe0d521ca1ae72decc06f1570aa43c781a2 (CryptoNaught)

Source: BscScan.com

Zoom 1m 6m 1y **All**

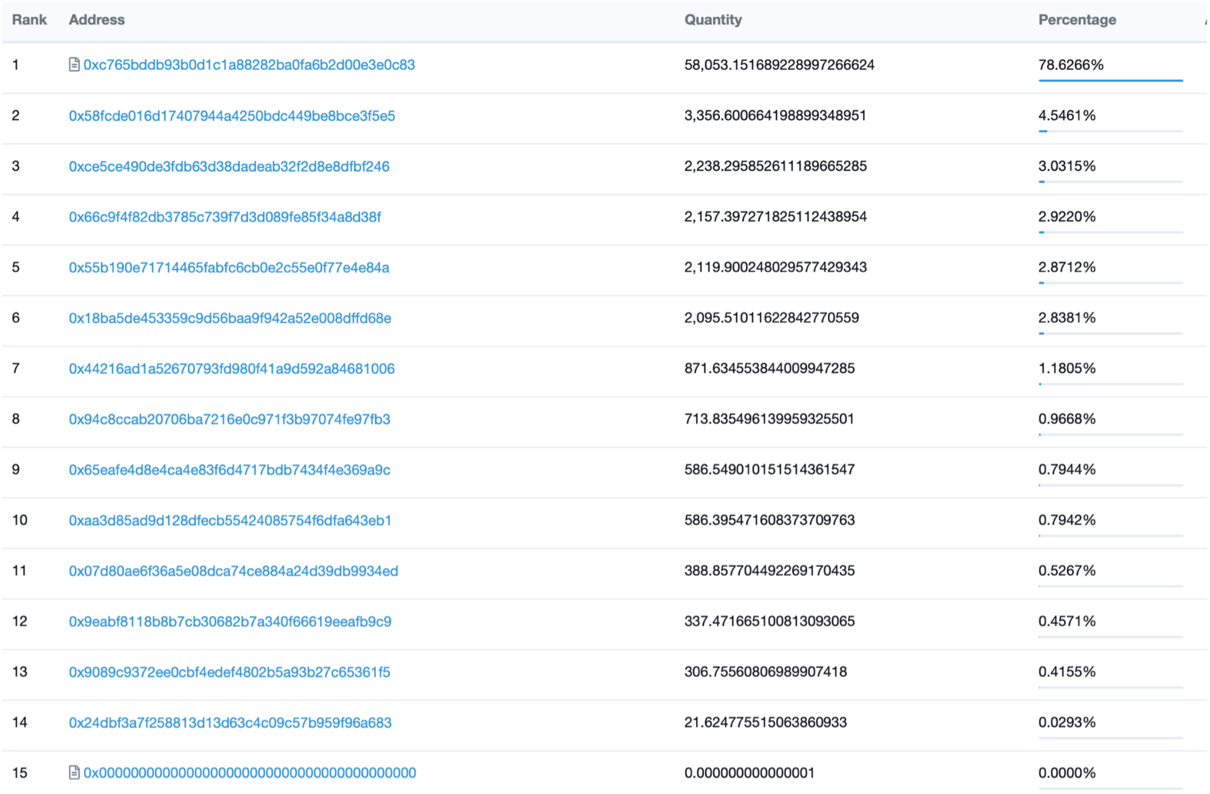
From May 2, 2021 To May 6, 2021

CryptoNaught top 10 token holders



Rank	Address	Quantity (Token)	Percentage
1	0xb82f3d9398ee279b0a4a88fa39e87605ea82c90f	91,250,189.889670631464714174	9.1250%
2	0xa70b82938c50172c28cbc1af8a476cdfd89770f3	37,034,481.651631788598469096	3.7034%
3	0xb6cc9f639d8e31391d1129719e7ce35cbc81ac9e	30,922,354.346750945749579371	3.0922%
4	0xbcf00e3dea3b0a587c68f072f43785c81dcfec40	24,479,769.978100987735306532	2.4480%
5	0x55b190e71714465fabfc6cb0e2c55e0f77e4e84a	22,495,051.916605493598382499	2.2495%
6	0x58fcde016d17407944a4250bdc449be8bce3f5e5	22,076,100.008235259926503322	2.2076%
7	0x153bbc0c41468abf2a7ed86d7cf4e875a52c67b8	20,584,452.389818687270326448	2.0584%
8	0xca352f10071cb90b951a361e5d95b2e35efafea1	20,497,265.19093746154384717	2.0497%
9	0x77d5dceedf2800964a6c059c0ef0f24ab4f0afe0	20,004,989.208674147586346659	2.0005%
10	0x44216ad1a52670793fd980f41a9d592a84681006	19,353,056.388028594122619231	1.9353%

CryptoNaught LP token holders



Rank	Address	Quantity	Percentage
1	0xc765bddb93b0d1c1a88282ba0fa6b2d00e3e0c83	58,053.151689228997266624	78.6266%
2	0x58fcde016d17407944a4250bdc449be8bce3f5e5	3,356.600664198899348951	4.5461%
3	0xce5ce490de3fdb63d38dadeab32f2d8e8dfbf246	2,238.295852611189665285	3.0315%
4	0x66c9f4f82db3785c739f7d3d089fe85f34a8d38f	2,157.397271825112438954	2.9220%
5	0x55b190e71714465fabfc6cb0e2c55e0f77e4e84a	2,119.900248029577429343	2.8712%
6	0x18ba5de453359c9d56baa9f942a52e008dffd68e	2,095.51011622842770559	2.8381%
7	0x44216ad1a52670793fd980f41a9d592a84681006	871.634553844009947285	1.1805%
8	0x94c8ccab20706ba7216e0c971f3b97074fe97fb3	713.835496139959325501	0.9668%
9	0x65eafe4d8e4ca4e83f6d4717bdb7434f4e369a9c	586.549010151514361547	0.7944%
10	0xaa3d85ad9d128dfecb55424085754f6dfa643eb1	586.395471608373709763	0.7942%
11	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	388.857704492269170435	0.5267%
12	0x9eabf8118b8b7cb30682b7a340f66619eeafb9c9	337.471665100813093065	0.4571%
13	0x9089c9372ee0cbf4edef4802b5a93b27c65361f5	306.75560806989907418	0.4155%
14	0x24dbf3a7f258813d13d63c4c09c57b959f96a683	21.624775515063860933	0.0293%
15	0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%

Contract functions details

```
+ [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

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

+ [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] geUnlockTime
  - [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] 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 #

+  CryptoNaught (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] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner
  - [Prv] _transferBothExcluded #
  - [Pub] excludeFromFee #
    - modifiers: onlyOwner
  - [Pub] includeInFee #
    - modifiers: onlyOwner
  - [Ext] setTaxFeePercent #
```

  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] enableTrading #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #

($) = 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

Note

Transfer function differs from the SafeMoon from which the project is forked. Always will be called the standard transfer even if some accounts are excluded from the rewards.

High Severity Issues

No high severity issues found.

Medium Severity Issues

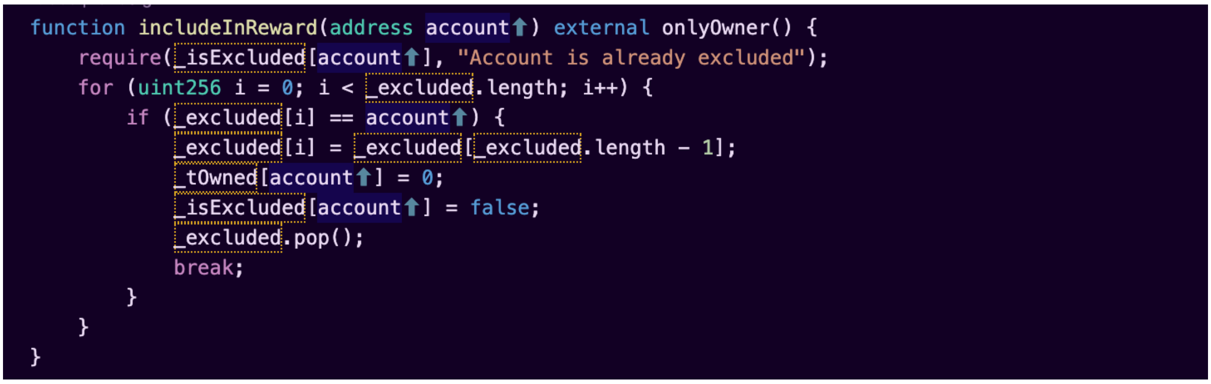
No medium severity issues found.

Low Severity Issues

1. Out of gas

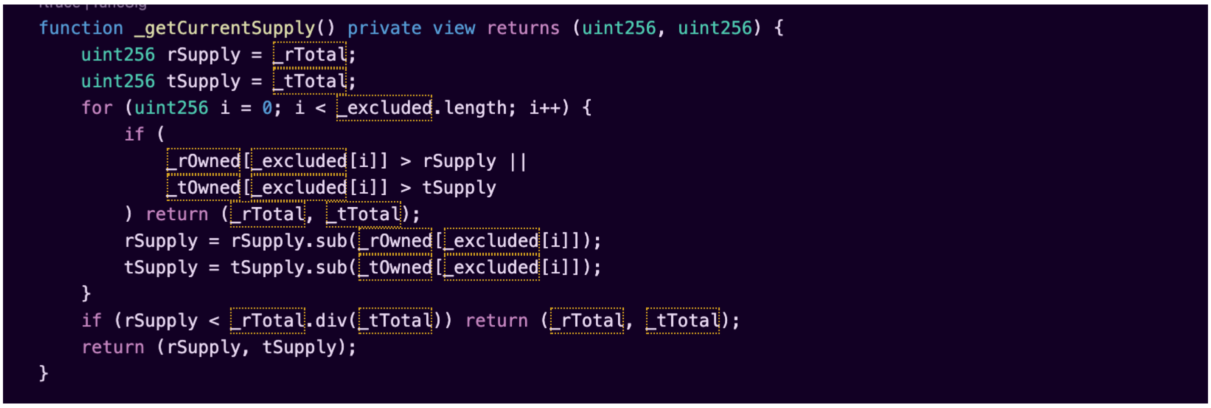
Issue:

- ❏ 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);
}
```

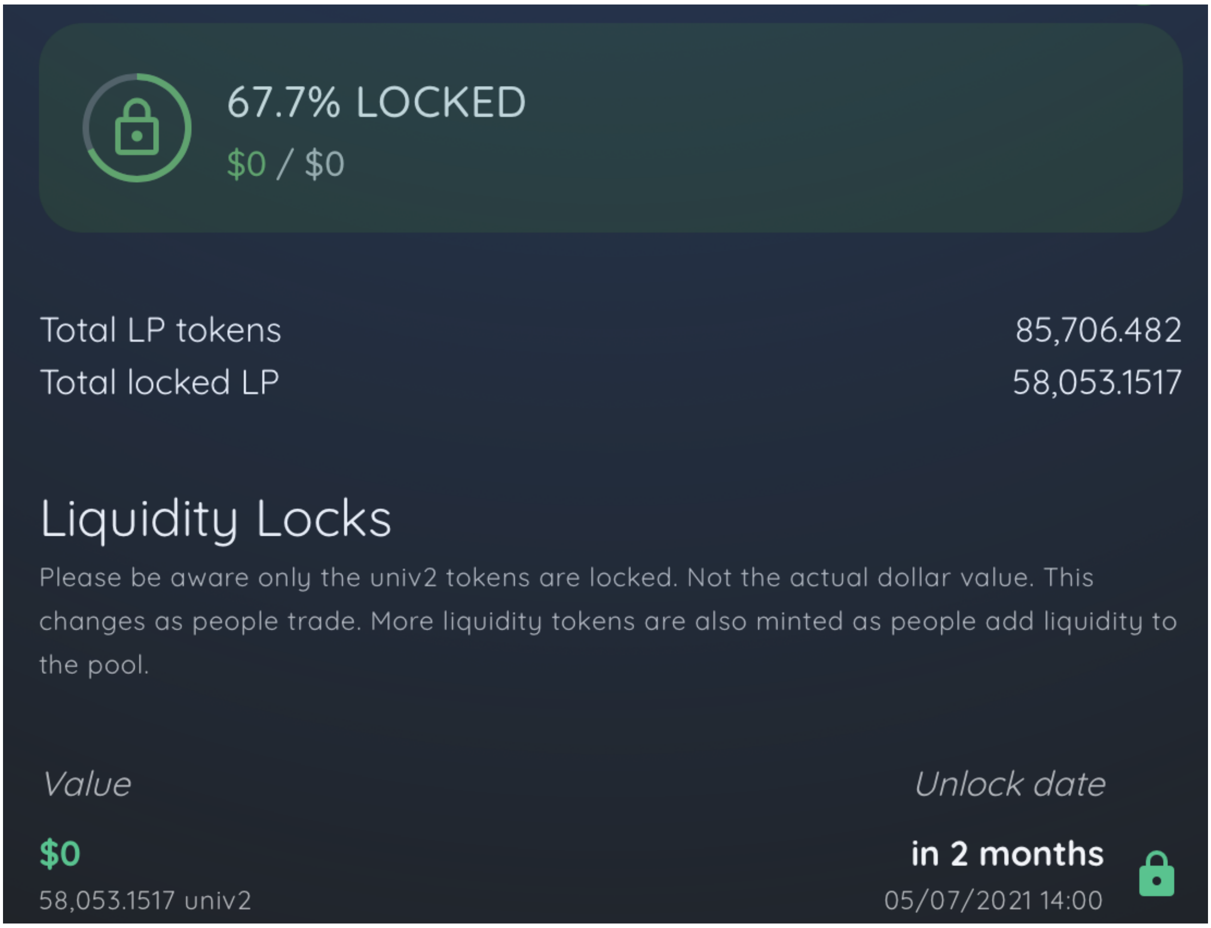
Recommendation:

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

Conclusion

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

Liquidity locking details provided by the team can be found by this link - https://unicrypt.network/amm/pancakev2/pair/0xb82f3d9398Ee279B0A4a88FA9E87605eA82c90f



67.7% LOCKED

$0 / $0

Total LP tokens 85,706.482

Total locked LP 58,053.1517

Liquidity Locks

Please be aware only the univ2 tokens are locked. Not the actual dollar value. This changes as people trade. More liquidity tokens are also minted as people add liquidity to the pool.

Value: $0 — 58,053.1517 univ2

Unlock date: in 2 months — 05/07/2021 14:00

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.