Smart Contract Security Audit

Audit details:

Audited project:	Secured MoonRat
Deployer address:	0xe2c3afa76a045e089fe99316e59fc2242bf7599f
Client contacts:	Secured MoonRat team
Blockchain:	Binance Smart Chain
Project website:	https://moonrat.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 Secured MoonRat to perform an audit of smart contracts:

- *https://bscscan.com/address/0x68590a47578e5060a29fd99654f4556dbfa05d10#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

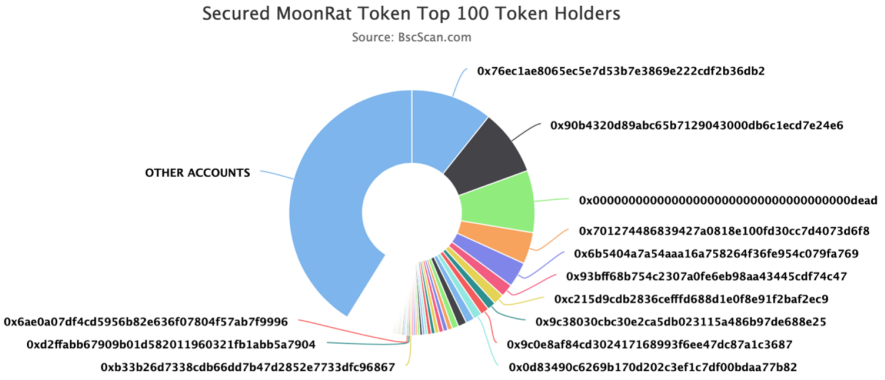
Token contract details for 02.05.2021.

Contract name:	Secured MoonRat
Contract address:	0x68590a47578e5060a29fd99654f4556dbfa05d10
Total supply:	1_000_000_000_000_000_000_000_000
Token ticker:	SMRAT
Decimals:	9
Token holders:	66548
Transactions count:	131985
Top 100 holders dominance:	58.82 %
Liquidity fee:	8
Tax fee:	2
Total fees:	10_011_875_717_576_235_581_617
Pancake pair:	0x90b4320d89abc65b7129043000db6c1ecd7e24e6
Contract deployer address:	0xe2c3afa76a045e089fe99316e59fc2242bf7599f
Contract's current owner address:	0x0000000000000000000000000000000000000000

Secured MoonRat token distribution

The top 100 holders collectively own 58.82%
(588,161,729,071,991.00 Tokens) of Secured MoonRat Token

Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 66,548

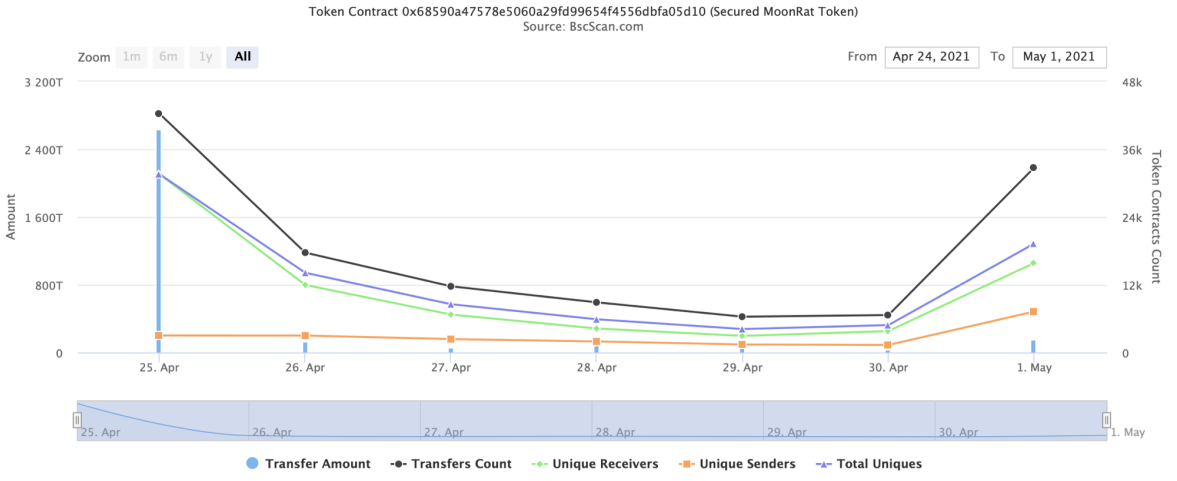


(A total of 588,161,729,071,991.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

Secured MoonRat contract interaction details

Time Series: Token Contract Overview

Sun 25, Apr 2021 - Sat 1, May 2021



Secured MoonRat top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x76ec1ae8065ec5e7d53b7e3869e222cdf2b36db2	107,216,819,199,075.615083425	10.7217%
2	0x90b4320d89abc65b7129043000db6c1ecd7e24e6	87,168,674,410,479.072206132	8.7169%
3	0x000000000000000000000000000000000000dead	81,855,684,484,354.028725366	8.1856%
4	0x701274486839427a0818e100fd30cc7d4073d6f8	41,673,023,282,875.213933102	4.1673%
5	0x6b5404a7a54aaa16a758264f36fe954c079fa769	33,201,490,392,990.711605714	3.3201%
6	0x93bff68b754c2307a0fe6eb98aa43445cdf74c47	16,863,879,819,923.934831395	1.6864%
7	0xc215d9cdb2836cefffd688d1e0f8e91f2baf2ec9	14,215,377,567,664.636222466	1.4215%
8	0x9c38030cbc30e2ca5db023115a486b97de688e25	11,215,214,611,784.999563524	1.1215%
9	0x9c0e8af84cd302417168993f6ee47dc87a1c3687	11,199,667,749,790.568210407	1.1200%
10	0x0d83490c6269b170d202c3ef1c7df00bdaa77b82	11,199,259,205,990.606631382	1.1199%

Secured MoonRat LP top 10 token holders

Rank	Address	Quantity	Percentage
1	0x000000000000000000000000000000000000dead	19,812.79256454644415855	88.7565%
2	0x0000000000000000000000000000000000000000	2,161.308146530746915517	9.6821%
3	Moon Rat: Deployer	264.180369402282296562	1.1835%
4	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	74.166346653942195675	0.3322%
5	0xb5c5541ddac0ef32f463a5718aba11000be01ce9	3.441428338121400695	0.0154%
6	0xa0d57cd806054568ce3bcaca9bc2d8e28a441e53	1.623930210624903649	0.0073%
7	0x9c38030cbc30e2ca5db023115a486b97de688e25	1	0.0045%
8	0x766acdddc7f67722fda400d5929fe548adb048f8	0.820589187224020367	0.0037%
9	0xb69529c62f307528aae309c5ab0573289290aeaa	0.553464754466876669	0.0025%
10	0x2afeb49dd7a0f86efdde06e1b6b0964ac8a9efc5	0.458132619527983421	0.0021%

Contract functions details

+ [Int] IBEP20
  - [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] IPancakeFactory

- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

+ [Int] IPancakePair
- [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] IPancakeRouter01
- [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] IPancakeRouter02 (IPancakeRouter01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Lib] Utils
  - [Prv] random
  - [Prv] isLotteryWon
  - [Pub] calculateBNBReward
  - [Pub] calculateTopUpClaim #
  - [Pub] swapTokensForEth #
  - [Pub] swapETHForTokens #
  - [Pub] addLiquidity #

+ ReentrancyGuard
  - [Pub] <Constructor> #

+ SecuredMoonRat (Context, IBEP20, Ownable, ReentrancyGuard)
  - [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
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Pub] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] setExcludeFromMaxTx # - modifiers: onlyOwner
- [Pub] calculateBNBReward
- [Pub] getRewardCycleBlock
- [Pub] claimBNBReward # - modifiers: isHuman,nonReentrant
- [Prv] topUpClaimCycleAfterTransfer #
- [Prv] ensureMaxTxAmount #
- [Pub] disruptiveTransfer ($)
- [Prv] swapAndLiquify #
- [Pub] activateContract # - modifiers: onlyOwner

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! Liquidity pair contract is not checked due to out of scope.

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.