Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

Parabolic

Deployer address

0x9f9a54e5f0c07db318bb27091ae398c15608603f

Client contacts:

Parabolic team

Blockchain

Binance Smart Chain

Project website:

https://parabolictoken.com

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 Parabolic to perform an audit of smart contracts:
https://bscscan.com/address/0xb5bcf4faa81457e98f4609a2a3291df64e246f01#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

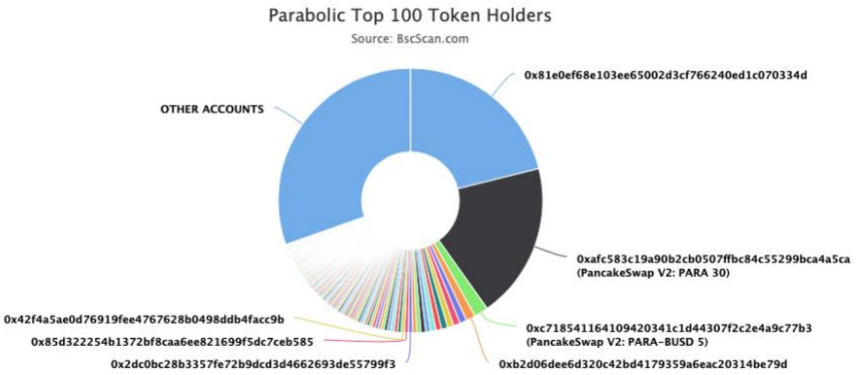
Token contract details for 05.10.2021

Contract name	Parabolic
Contract address	0xB5bCF4fAa81457e98f4609a2a3291dF64E246f01
Total supply	947,095,620,535.59797
Token ticker	PARA
Decimals	9
Token holders	9,660
Transactions count	55,049
Top 100 holders dominance	69.61%
Liquidity fee	30
Reflection fee	0
Burn fee	30
External fee	60
Total fees collected	0
Pancake V2 pair	0xafc583c19a90b2cb0507ffbc84c55299bca4a5ca
Contract deployer address	0x9f9a54e5f0c07db318bb27091ae398c15608603f
Contract's current owner address	0x9f9a54e5f0c07db318bb27091ae398c15608603f

Parabolic Token Distribution

The top 100 holders collectively own 69.61% (659,257,284,185.62 Tokens) of Parabolic

Token Total Supply: 947,095,620,535.60 Token | Total Token Holders: 9,660

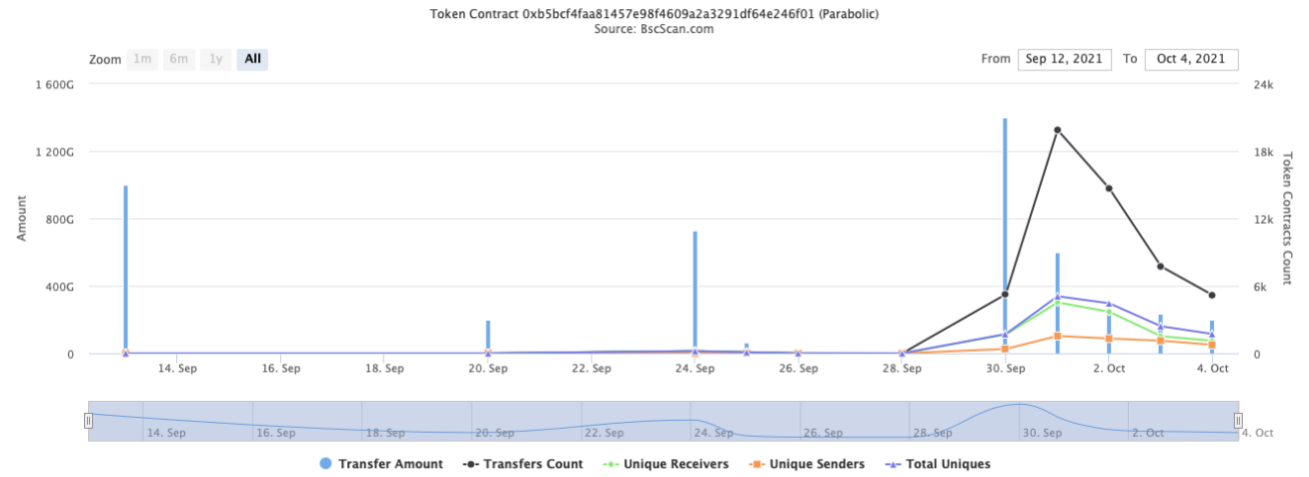


(A total of 659,257,284,185.62 tokens held by the top 100 accounts from the total supply of 947,095,620,535.60 token)

Parabolic Contract Interaction Details

Time Series: Token Contract Overview

Mon 13, Sept 2021 - Mon 4, Oct 2021



Parabolic Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x81e0ef68e103ee65002d3cf766240ed1c070334d	200,000,758,697.12616557	21.1173%
2	PancakeSwap V2: PARA 30	180,465,633,866.579864459	19.0546%
3	PancakeSwap V2: PARA-BUSD 5	16,253,034,887.406842762	1.7161%
4	0xb2d06dee6d320c42bd4179359a6eac20314be79d	10,765,760,084.472883576	1.1367%
5	0xef6c9261175d8dad2bd03af7172acda1474f5039	8,167,530,876.7899241	0.8624%
6	0xe31bbfd345284d3e2dd421e674ec4434da9b4e50	7,677,401,768.288044271	0.8106%
7	0x7797d0bb907904a611024b1cf95a9998626a5140	7,289,215,564.643217368	0.7696%
8	0x1033affd2e196e1fb79ed5ef74413f512b9beed7	7,240,684,405.778031866	0.7645%
9	0x9ee562e9319857a8bc2b92b5d769bcc696bbbfda	6,423,046,017.045399052	0.6782%
10	0xf93c8838c2a6f35cc713eac9740a0fc24f108adf	6,121,611,170.481252475	0.6464%

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)
  - [Pub] <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 #

+ Parabolic (Context, IBEP20, 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] totalFeesCollected
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Int] _burn #
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Pub] excludedFromMaxTxAmount #
  - modifiers: onlyOwner
- [Pub] includeInMaxTxAmount #
  - modifiers: onlyOwner
- [Pub] excludedFromExternalTokenMinAmount #
  - modifiers: onlyOwner
- [Pub] includeInExternalTokenMinAmount #
  - modifiers: onlyOwner
- [Pub] excludedFromAntiWhale #
  - modifiers: onlyOwner
- [Pub] includeInAntiWhale #
  - modifiers: onlyOwner
- [Ext] setBurnFeePercent #
  - modifiers: onlyOwner
- [Ext] setExternalFeePercent #
  - modifiers: onlyOwner
- [Ext] setReflectFeePercent #
  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxTokensSell #
  - modifiers: onlyOwner
- [Ext] setMaxTxTokensBuy #
  - modifiers: onlyOwner

- [Ext] setMaxTokenPerAddress #
  - modifiers: onlyOwner
- [Ext] setExternalTokenMinAmount #
  - modifiers: onlyOwner
- [Ext] setExternalAddress #
  - modifiers: onlyOwner
- [Ext] setLiquidityAddress #
  - modifiers: onlyOwner
- [Pub] setTransactionlockTime #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Pub] excludedFromTransactionlock #
  - modifiers: onlyOwner
- [Pub] includeInTransactionlock #
  - modifiers: onlyOwner
- [Pub] getIsExcludedFromTransactionlock
- [Ext] <Fallback> ($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateBurnFee
- [Prv] calculateReflectionFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Pub] setMinTokensSellToAndTransfer #
  - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferFromExcluded #
- [Prv] _transferToExcluded #
- [Prv] _transferStandard #
- [Prv] _transferBothExcluded #
- [Pub] blacklistSingleWallet #
  - modifiers: onlyOwner
- [Pub] blacklistMultipleWallets #
  - modifiers: onlyOwner
- [Pub] isBlacklisted
- [Ext] unBlacklistSingleWallet #
  - modifiers: onlyOwner
- [Pub] unBlacklistMultipleWallets #
  - modifiers: onlyOwner
- [Ext] setExternalToken #
  - modifiers: onlyOwner

- [Ext] setIsExternalTokenHoldEnabaled #
  - modifiers: onlyOwner
- [Ext] burnTokens #
- [Pub] recoverBNB #
  - modifiers: onlyOwner
- [Pub] setRouterAddress #
  - 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.	Low issues
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.

2. Burn event issue

Issue:

- The function _burn and burnTokens emits transferring burn amount from address to burn to contract address. This is wrong event, there is not transferring tokens to contract address.

Recommendation:

Change burn event.

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

- Owner can change the reflection fee, external fee, burn fee and liquidity fee.
- Owner can change the maximum transaction amount.
- Owner can exclude from the maximum transaction amount.
- Owner can exclude from the external token min amount.
- Owner can exclude from the transaction lock.
- Owner can exclude from the antiwhale.
- Owner can exclude from the fees.
- Owner can change _maxTxAmountBuy and _maxTxAmountSell.
- Owner can change charity and autoLiquidityReceiver address.
- Owner can change max tokens per address.
- Owner can change _externalTokenMinAmount.
- Owner can change external address.
- Owner can change transaction lock time.
- Owner can change charity address.
- Owner can change _numTokensSellToAndTransfer.
- Owner can change blacklist wallets.
- Owner can change external tokens.
- Owner can change isExternalTokenHoldEnabled value.
- Owner can withdraw contract BNBs.
- Owner can change router address.

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/v3/dxlplocksearch?id=0&add=0xB5bCF4fAa81457e98f4609a2a3291dF64E246f01&type=lpdefi&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.