Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details

Audited project

BinosaursToken

Deployer address

0xf50afc2ac59202c5618b32d36bb9a68180cbf1c0

Client contacts:

BinosaursToken team

Blockchain

Binance Smart Chain

Project website:

https://binosaurs.io/

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 BinosaursToken to perform an audit of smart contracts:

https://bscscan.com/address/0x7fdd003d3b61dda10429c1ebb502ec02946219cc#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

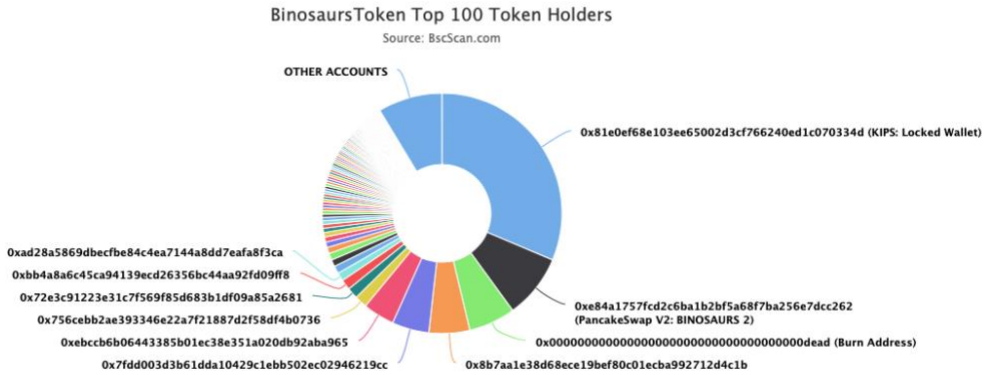
Token contract details for 14.11.2021

Contract name	BinosaursToken
Contract address	0x7fDd003D3B61dDA10429C1EbB502Ec02946219cc
Total supply	1,000,000,000
Token ticker	BINOSAURS
Decimals	9
Token holders	1,580
Transactions count	13,416
Top 100 holders dominance	91.33%
Total fees	4
Pair	0xe84a1757fcd2c6ba1b2bf5a68f7ba256e7dcc262
Contract deployer address	0xf50afc2ac59202c5618b32d36bb9a68180cbf1c0
Contract's current owner address	0xf50afc2ac59202c5618b32d36bb9a68180cbf1c0

BinosaursToken Token Distribution

The top 100 holders collectively own 91.33% (913,308,155.89 Tokens) of BinosaursToken

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 1,580

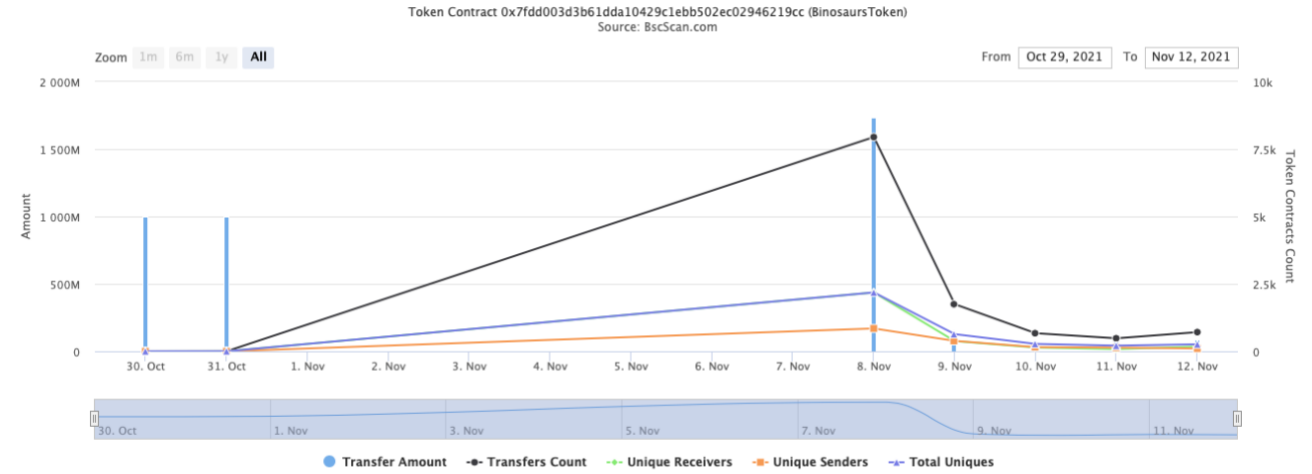


(A total of 913,308,155.89 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

BinosaursToken Contract Interaction Details

Time Series: Token Contract Overview

Sat 30, Oct 2021 - Fri 12, Nov 2021



BinosaursToken Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	KIPS: Locked Wallet	313,500,000	31.3500%
2	PancakeSwap V2: BINOSAURS 2	86,306,601.14333523	8.6307%
3	Burn Address	62,977,101.18467866	6.2977%
4	0x8b7aa1e38d68ece19bef80c01ecba992712d4c1b	54,872,516.258256149	5.4873%
5	0x7fdd003d3b61dda10429c1ebb502ec02946219cc	50,055,821.135618042	5.0056%
6	0xebccb6b06443385b01ec38e351a020db92aba965	42,431,110.204467274	4.2431%
7	0x756cebb2ae393346e22a7f21887d2f58df4b0736	16,950,660.160857367	1.6951%
8	0x72e3c91223e31c7f569f85d683b1df09a85a2681	14,722,492.272827939	1.4722%
9	0xbb4a8a6c45ca94139ecd26356bc44aa92fd09ff8	13,999,983.569452127	1.4000%
10	0xad28a5869dbecfbe84c4ea7144a8dd7eafa8f3ca	11,223,089.21029112	1.1223%

Contract functions details

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

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals

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

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

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

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

+ [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 #

+ ERC20 (Context, IERC20, IERC20Metadata)
- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol

  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _beforeTokenTransfer #

+ BinosaursToken (ERC20, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Pub] updateUniswapV2Router #
    - modifiers: onlyOwner
  - [Pub] transfer #
  - [Pub] Batchtransfer #
  - [Pub] excludeFromFees #
    - modifiers: onlyOwner
  - [Pub] includeInFees #
    - modifiers: onlyOwner
  - [Ext] setSwapTokensAtAmount #
    - modifiers: onlyOwner
  - [Pub] updateMarketingWallet #
    - modifiers: onlyOwner
  - [Pub] isExcludedFromFees
  - [Int] _transfer #
  - [Prv] sendToWallet #
  - [Ext] getBalance
  - [Prv] swapTokensForBNB #
  - [Ext] withdrawTokens #
    - modifiers: onlyOwner
  - [Ext] goLive #
    - 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 `Batchtransfer()` uses the loop to transfer for multiple accounts. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

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

- Owner can change Uniswap router.
- Owner can include in and exclude from fee.
- Owner can change token amount to start swap.
- Owner can update marketing address.
- Owner can withdraw ERC20 tokens.
- Owner can launch contract.

Conclusion

Smart contracts contain low severity issues and owner privileges. 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=0x7fDd003D3B61dDA10429C1EbB502Ec02946219cc&type=lpdefi&chain=BSC
https://dxsale.app/app/v3/dxtokenlocksearch?id=0&add=0x7fDd003D3B61dDA10429C1EbB502Ec02946219cc&type=tokenlock&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.