TechRate

Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	BuckSwap
Deployer address	0x425497f3a908f0e9337f68c061755c0f5669cb3f
Blockchain:	Binance Smart Chain
Project website:	https://buckswap.io

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 BuckSwap to perform an audit of smart contracts:

- *https://bscscan.com/address/0xe8aAb7213eE05091A81eE29206Ec1191A4Ed1381#code*
- *https://bscscan.com/address/0xDA28B68483c44F563168b6e4b7Df9209a02ed64E#code*
- *https://bscscan.com/address/0xD8d0BA506d86EfA534BF7ceB6abA7Dd36941670A*

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.

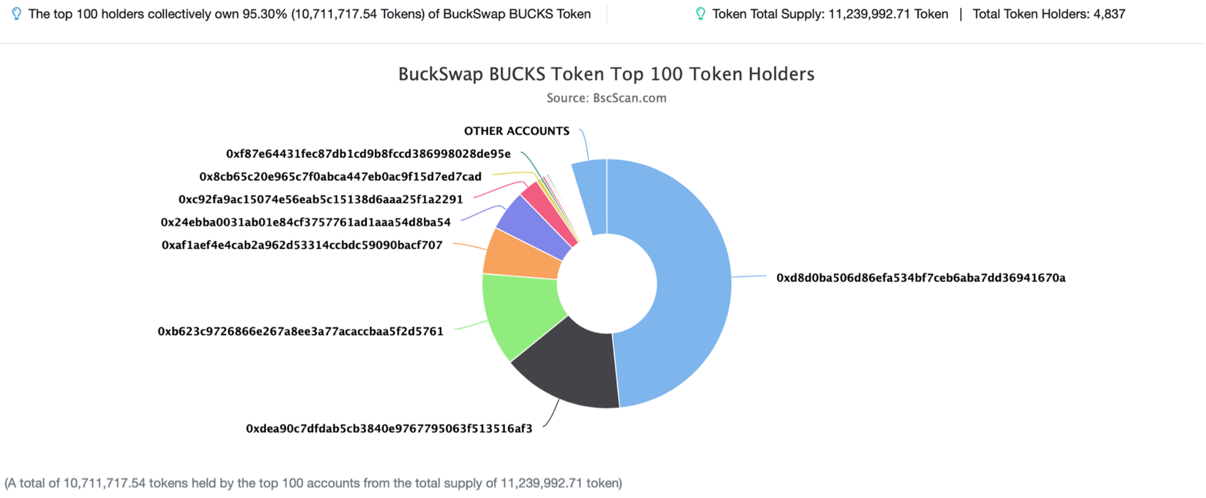
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 11.05.2021.

Contract name:	BuckSwap
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0xDA28B68483c44F563168b6e4b7Df9209a02ed64E
Total supply:	112401389329787234040163137
Token ticker:	BUCKS
Decimals:	18
Token holders:	4837
Transactions count:	55886
Top 100 dominance:	95.3 %
Contract deployer address:	0x425497f3a908f0e9337f68c061755c0f5669cb3f
Contract’s current owner address:	0xd8d0ba506d86efa534bf7ceb6aba7dd36941670a

BuckSwap token distribution



The top 100 holders collectively own 95.30% (10,711,717.54 Tokens) of BuckSwap BUCKS Token

Token Total Supply: 11,239,992.71 Token | Total Token Holders: 4,837

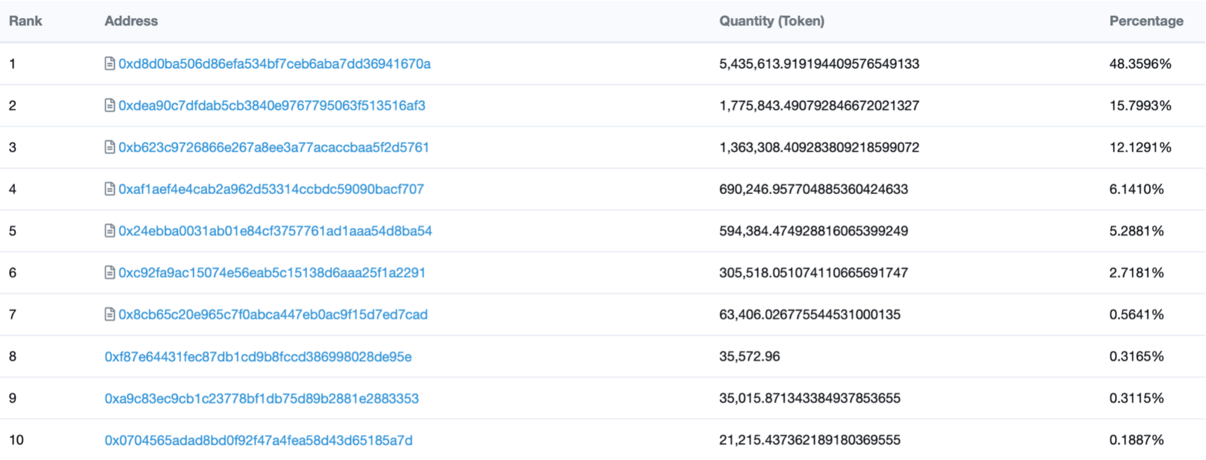
BuckSwap BUCKS Token Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xf87e64431fec87db1cd9b8fccd386998028de95e
0x8cb65c20e965c7f0abca447eb0ac9f15d7ed7cad
0xc92fa9ac15074e56eab5c15138d6aaa25f1a2291
0x24ebba0031ab01e84cf3757761ad1aaa54d8ba54
0xaf1aef4e4cab2a962d53314ccbdc59090bacf707
0xd8d0ba506d86efa534bf7ceb6aba7dd36941670a
0xb623c9726866e267a8ee3a77acaccbaa5f2d5761
0xdea90c7dfdab5cb3840e9767795063f513516af3

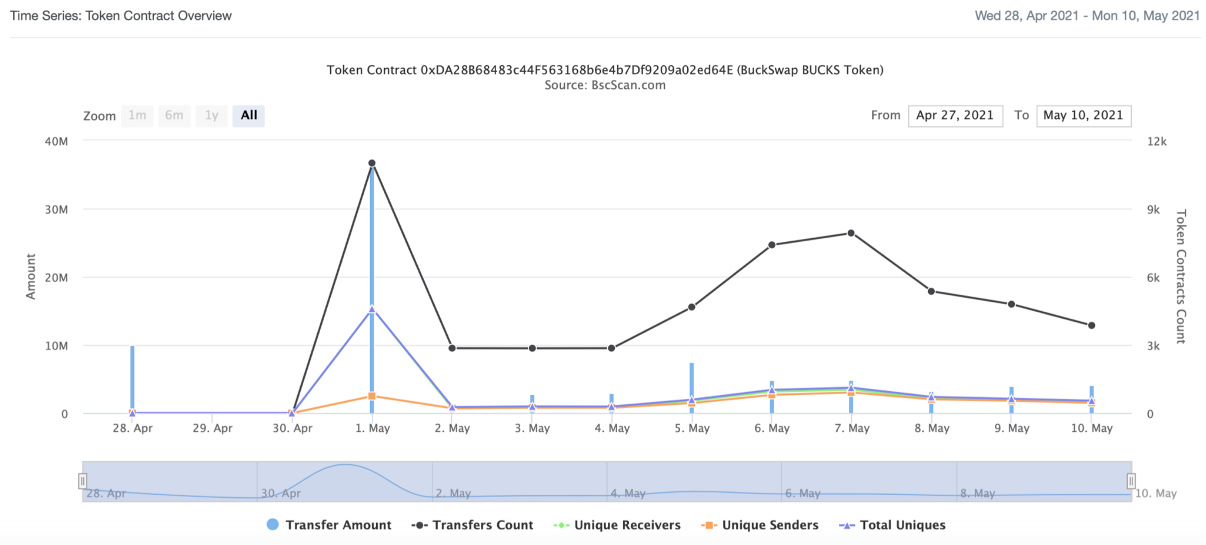
(A total of 10,711,717.54 tokens held by the top 100 accounts from the total supply of 11,239,992.71 token)

BuckSwap top 10 token holders



Rank	Address	Quantity (Token)	Percentage
1	0xd8d0ba506d86efa534bf7ceb6aba7dd36941670a	5,435,613.919194409576549133	48.3596%
2	0xdea90c7dfdab5cb3840e9767795063f513516af3	1,775,843.490792846672021327	15.7993%
3	0xb623c9726866e267a8ee3a77acaccbaa5f2d5761	1,363,308.409283809218599072	12.1291%
4	0xaf1aef4e4cab2a962d53314ccbdc59090bacf707	690,246.957704885360424633	6.1410%
5	0x24ebba0031ab01e84cf3757761ad1aaa54d8ba54	594,384.474928816065399249	5.2881%
6	0xc92fa9ac15074e56eab5c15138d6aaa25f1a2291	305,518.051074110665691747	2.7181%
7	0x8cb65c20e965c7f0abca447eb0ac9f15d7ed7cad	63,406.026775544531000135	0.5641%
8	0xf87e64431fec87db1cd9b8fccd386998028de95e	35,572.96	0.3165%
9	0xa9c83ec9cb1c23778bf1db75d89b2881e2883353	35,015.871343384937853655	0.3115%
10	0x0704565adad8bd0f92f47a4fea58d43d65185a7d	21,215.437362189180369555	0.1887%

BuckSwap transaction details



Time Series: Token Contract Overview

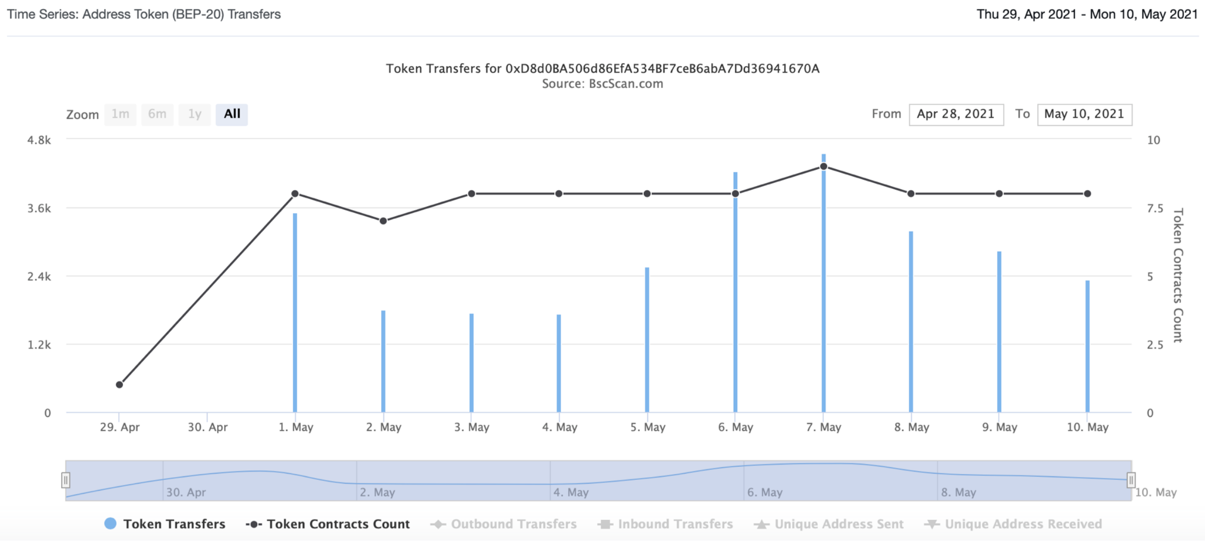
Wed 28, Apr 2021 - Mon 10, May 2021

Token Contract 0xDA28B68483c44F563168b6e4b7Df9209a02ed64E (BuckSwap BUCKS Token)
Source: BscScan.com

Zoom 1m 6m 1y All

From Apr 27, 2021 To May 10, 2021

BucksMaster transaction details



Time Series: Address Token (BEP-20) Transfers

Thu 29, Apr 2021 - Mon 10, May 2021

Token Transfers for 0xD8d0BA506d86EfA534BF7ceB6abA7Dd36941670A
Source: BscScan.com

Zoom 1m 6m 1y All

From Apr 28, 2021 To May 10, 2021

BucksMaster contract details for 11.05.2021.

Contract name:	MasterChef
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0xD8d0BA506d86EfA534BF7ceB6abA7Dd36941670A
Deployer address:	0x425497f3a908f0e9337f68c061755c0f5669cb3f
Fee address:	0x83c023eba68ca6ea2f528359bcdba409321925fc
Dev address:	0x4caf15415a4017c326f2fa8b7ba921d3618a8c94
BUCKS contract address:	0xda28b68483c44f563168b6e4b7df9209a02ed64e
BUCKS per block:	3000000000000000000
Contract owner address:	0xe8aab7213ee05091a81ee29206ec1191a4ed1381
Pool length:	8
Start block:	7030500
Total alloc point:	235
Bonus multiplier:	1

MasterChef functions outline

+ [Lib] SafeMath

  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod
  - [Int] min
  - [Int] sqrt

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ [Lib] SafeBEP20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ Context
  - [Int] <Constructor> #
  - [Int] _msgSender
  - [Int] _msgData

+ Ownable (Context)
  - [Int] <Constructor> #

```
  - [Pub] owner
  - [Pub] renounceOwnership #
     - modifiers: onlyOwner
  - [Pub] transferOwnership #
     - modifiers: onlyOwner
  - [Int] _transferOwnership #

+  BEP20 (Context, IBEP20, Ownable)
  - [Pub] <Constructor> #
  - [Ext] getOwner
  - [Pub] name
  - [Pub] decimals
  - [Pub] symbol
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] mint #
     - modifiers: onlyOwner
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _burnFrom #

+  BucksToken (BEP20)
  - [Pub] mint #
     - modifiers: onlyOwner
  - [Ext] delegates
  - [Ext] delegate #
  - [Ext] delegateBySig #
  - [Ext] getCurrentVotes
  - [Ext] getPriorVotes
  - [Int] _delegate #
  - [Int] _moveDelegates #
  - [Int] _writeCheckpoint #
  - [Int] safe32
  - [Int] getChainId

+  BucksMaster (Ownable)
  - [Pub] <Constructor> #
  - [Ext] poolLength
  - [Pub] add #
```

    - modifiers: onlyOwner
  - [Pub] set #
    - modifiers: onlyOwner
  - [Pub] getMultiplier
  - [Ext] pendingBucks
  - [Pub] massUpdatePools #
  - [Pub] updatePool #
  - [Pub] deposit #
  - [Pub] withdraw #
  - [Pub] emergencyWithdraw #
  - [Int] safeBucksTransfer #
  - [Pub] dev #
  - [Pub] setFeeAddress #
  - [Pub] setDevFundPercentage #
  - [Pub] updateMiningRate #
    - 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. Block gas limit

Issue:

The updateMiningRate function can fail due to block gas limit if the pool size is too big.

2. add function issue

Issue:

If some LP token is added to the contract twice using function add, then the total amount of reward bucksReward in function updatePool will be incorrect.

Recommendation:

Add the mapping from address to bool and check that same address will not be added twice.

Owner privileges

❏ Dev address can change the dev fund percentage.

Conclusion

Smart contracts do not contain high severity issues! Audited only the three contracts listed above, pools and other contracts of the project are not audited.

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.