TechRate
Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	BICHON TOKENT
Deployer address:	0x7a5c911236917b483cdb3ea3090add8b23774888
Client contacts:	BICHON TOKENT team
Blockchain:	Binance Smart Chain
Project website:	https://bichontoken.com

April, 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 BICHON TOKENT to perform an audit of smart contracts:

- *https://bscscan.com/address/0xdf394853d830424cafccf7be7df065366cf31a69#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.

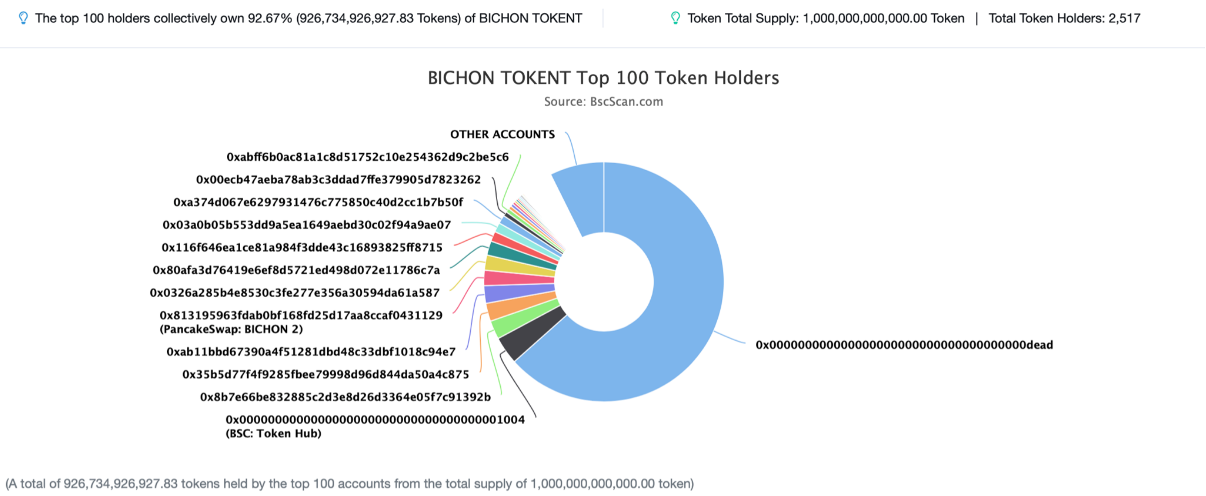
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 26.04.2021.

Contract name:	BICHON TOKENT
Contract address:	0xdf394853d830424cafccf7be7df065366cf31a69
Total supply:	1_000_000_000_000_000_000_000
Token ticker:	BICHON
Decimals:	9
Token holders:	2517
Transactions count:	10344
Top 100 holders dominance:	92.67 %
Tax fee:	9
Total fees:	199_398_213_664_730_648_658
Contract deployer address:	0x7a5c911236917b483cdb3ea3090add8b23774888
Contract’s current owner address:	0x7a5c911236917b483cdb3ea3090add8b23774888

BICHON TOKENT token distribution



The top 100 holders collectively own 92.67% (926,734,926,927.83 Tokens) of BICHON TOKENT

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 2,517

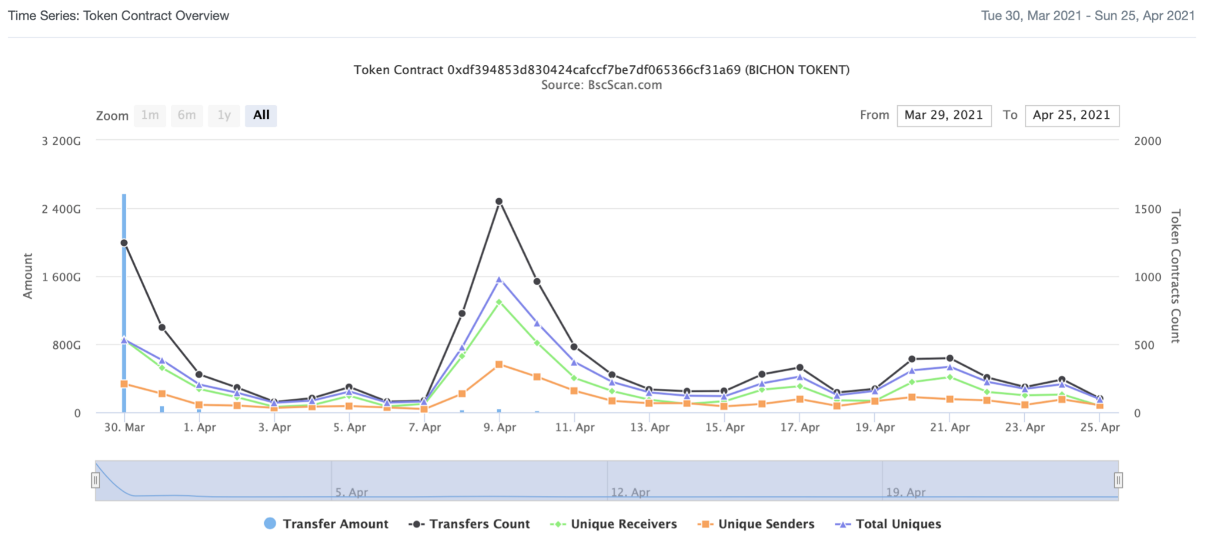
BICHON TOKENT Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xabff6b0ac81a1c8d51752c10e254362d9c2be5c6
0x00ecb47aeba78ab3c3ddad7ffe379905d7823262
0xa374d067e6297931476c775850c40d2cc1b7b50f
0x03a0b05b553dd9a5ea1649aebd30c02f94a9ae07
0x116f646ea1ce81a984f3dde43c16893825ff8715
0x80afa3d76419e6ef8d5721ed498d072e11786c7a
0x0326a285b4e8530c3fe277e356a30594da61a587
0x813195963fdab0bf168fd25d17aa8ccaf0431129 (PancakeSwap: BICHON 2)
0xab11bbd67390a4f51281dbd48c33dbf1018c94e7
0x35b5d77f4f9285fbee79998d96d844da50a4c875
0x8b7e66be832885c2d3e8d26d3364e05f7c91392b
0x0000000000000000000000000000000000001004 (BSC: Token Hub)
0x000000000000000000000000000000000000dead

(A total of 926,734,926,927.83 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

BICHON TOKENT contract interaction details



Time Series: Token Contract Overview

Tue 30, Mar 2021 - Sun 25, Apr 2021

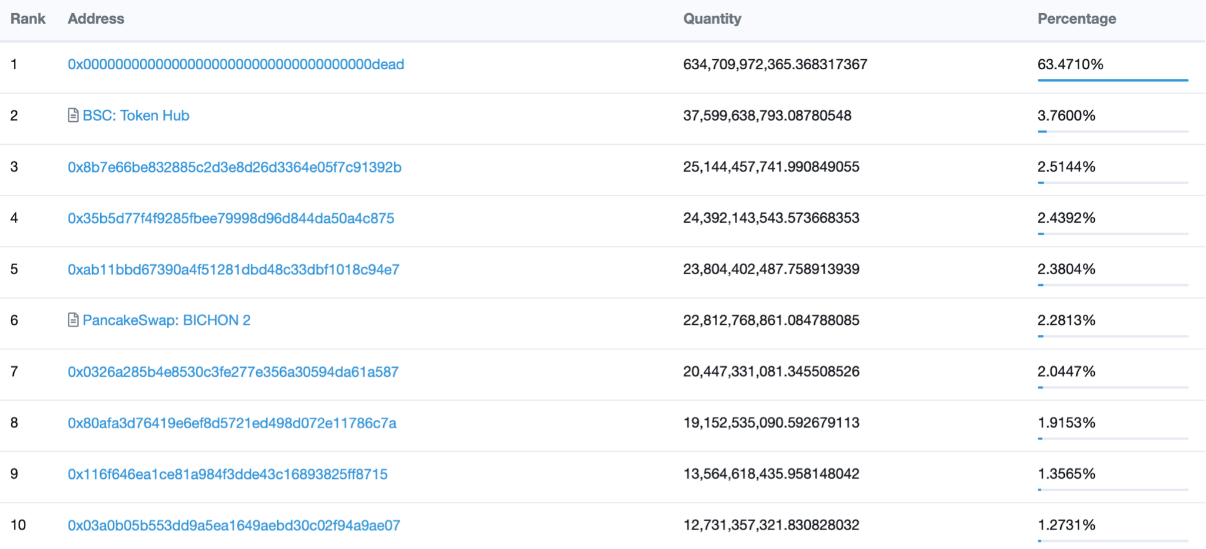
Token Contract 0xdf394853d830424cafccf7be7df065366cf31a69 (BICHON TOKENT)

Source: BscScan.com

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

From Mar 29, 2021 To Apr 25, 2021

BICHON TOKENT top 10 token holders



Rank	Address	Quantity	Percentage
1	0x000000000000000000000000000000000000dead	634,709,972,365.368317367	63.4710%
2	📄 BSC: Token Hub	37,599,638,793.08780548	3.7600%
3	0x8b7e66be832885c2d3e8d26d3364e05f7c91392b	25,144,457,741.990849055	2.5144%
4	0x35b5d77f4f9285fbee79998d96d844da50a4c875	24,392,143,543.573668353	2.4392%
5	0xab11bbd67390a4f51281dbd48c33dbf1018c94e7	23,804,402,487.758913939	2.3804%
6	📄 PancakeSwap: BICHON 2	22,812,768,861.084788085	2.2813%
7	0x0326a285b4e8530c3fe277e356a30594da61a587	20,447,331,081.345508526	2.0447%
8	0x80afa3d76419e6ef8d5721ed498d072e11786c7a	19,152,535,090.592679113	1.9153%
9	0x116f646ea1ce81a984f3dde43c16893825ff8715	13,564,618,435.958148042	1.3565%
10	0x03a0b05b553dd9a5ea1649aebd30c02f94a9ae07	12,731,357,321.830828032	1.2731%

Contract functions details

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

+ [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

+ [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

+  BICHON (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] isExcluded
- [Pub] totalFees
- [Pub] reflect #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
    - modifiers: onlyOwner
- [Ext] includeAccount #
    - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply

($) = 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

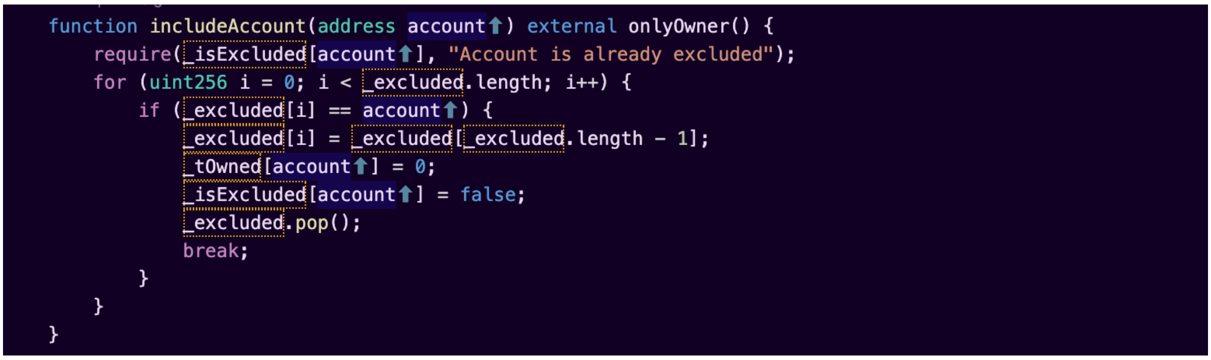
No medium severity issues found.

Low Severity Issues

1. Out of gas

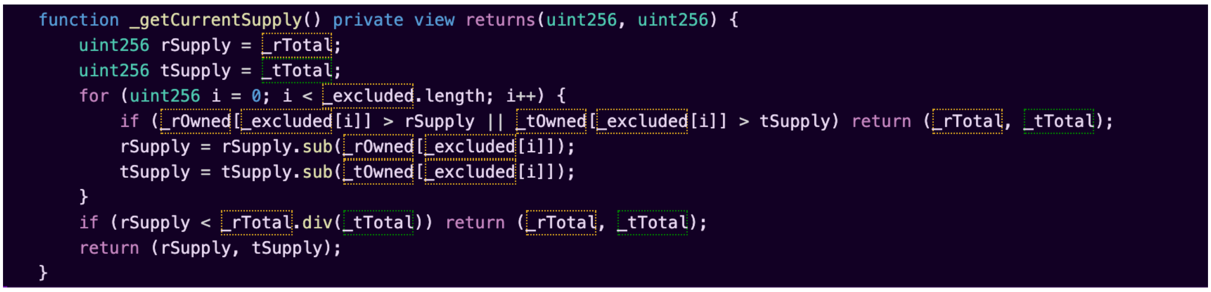
Issue:

- The function includeAccount() 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 includeAccount(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 only low severity issues.

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.