HackSafe

Smart Contract Security Audit Report

Buccaneer

April **2022**

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
Buccaneer

Deployer address
0xe4C25E73Cc7A2C0a69716b35E0f600a5be3a0816

Client contacts
Buccaneer team

Blockchain
Binance smart chain

Website
Not Provided

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) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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

HeckSafe was commissioned by Buccaneer to perform an audit of smart contracts:

- https://etherscan.io/address/0x831467b7B6BF9C705dC87899d48b57eE55C8d5cc#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issue 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

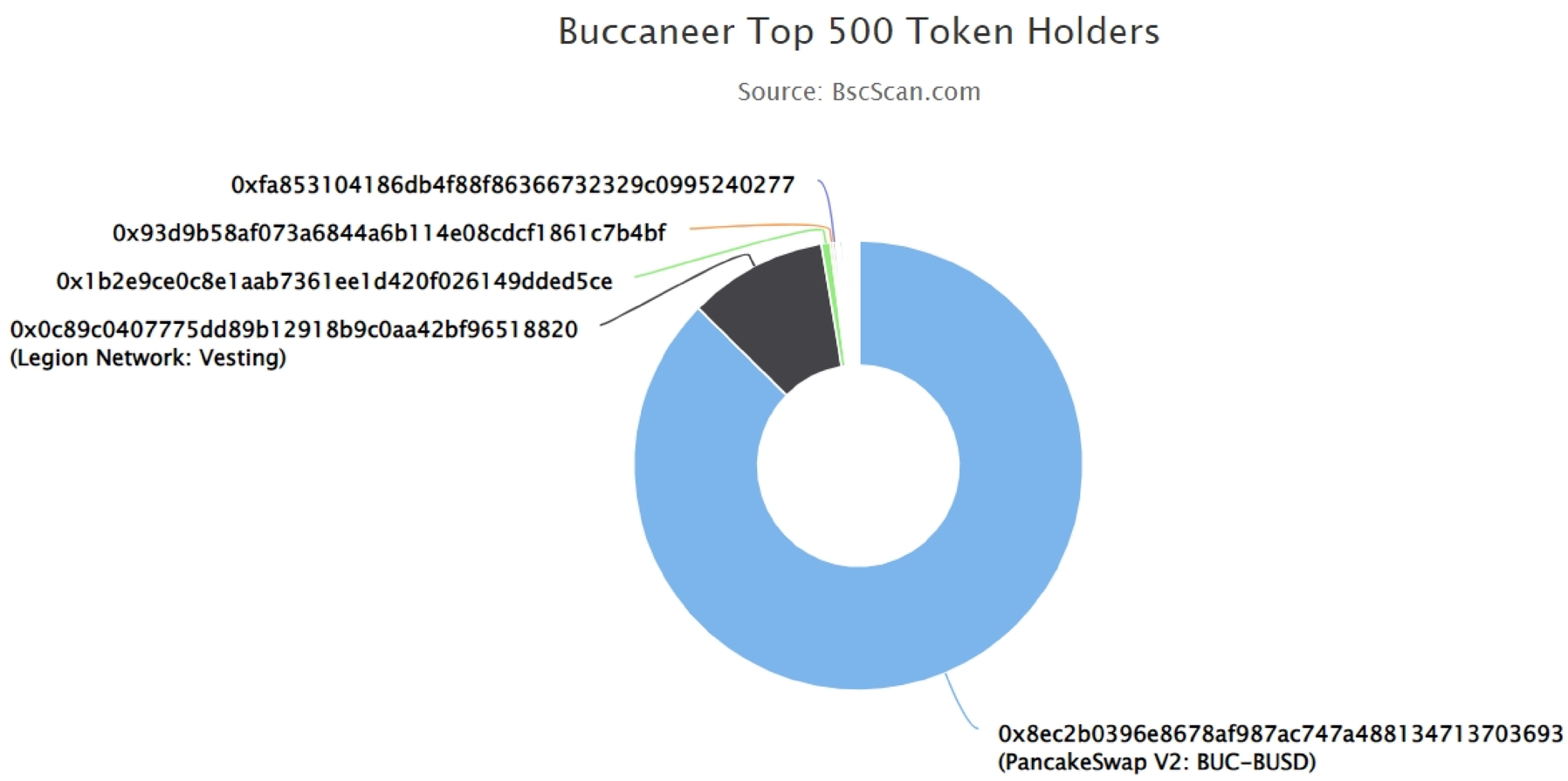
Token contract details for 14.04.2022

Contract name	: Buccaneer
Contract address	: 0x831467b7B6BF9C705dC87899d48b57eE55C8d5cc
Total supply	: 200000000 on deployment
Token Ticker	: BUC
Decimals	: 18
Network	: BSCScan
Transactions count	: 7,156
Token Holders	: 744 addresses
Contract deployer address	: 0xe4C25E73Cc7A2C0a69716b35E0f600a5be3a0816
Owner address	: 0xF2750f65F2e7da1834d2a65E1528E0c8da9C07a8

Buccaneer Token Distribution

The top 500 holders collectively own 100.00% (999,646,280.46 Tokens) of Buccaneer

Token Total Supply: 999,648,412.88 Token | Total Token Holders: 7



Buccaneer Top 10 Token Holders

(A total of 990,783,058.31 tokens held by the top 10 accounts from the total supply of 999,648,412.88 token)

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: BUC-BUSD	873,359,450.539625654913605771	87.3667%
2	Legion Network: Vesting	100,000,000	10.0035%
3	0x1b2e9ce0c8e1aab7361ee1d420f026149dded5ce	6,278,646.725309564167336219	0.6281%
4	0x93d9b58af073a6844a6b114e08cdcf1861c7b4bf	1,999,998	0.2001%
5	0xfa853104186db4f88f86366732329c0995240277	1,870,654.667046489157096638	0.1871%
6	0xdda56d1b9908f11b6dc60d0bcca8d7a6db9a58e4	1,632,282.888363003513794569	0.1633%
7	0x994d15055962d91c8ca830619c6cf5371f999999	1,627,697.227838176309746771	0.1628%
8	0x7b1229b4cc05d28d1ae8eba3d0bdecce674839ea	1,624,930	0.1626%
9	0x7daa9bc6d8a5b0955ddc40708a9e85c8a59d6d0d	1,305,516	0.1306%
10	0x5a377ebac2cecf65b5f4591b056a0756876534ee	1,083,882.26375430789399384	0.1084%

Contract functions details

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

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

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

+ Ownable (Context)
    - <constructor>
    - [Pub] owner
    - [Pub] renounceOwnership
        - Modifier: onlyOwner
    - [Pub] transferOwnership
        - Modifier: onlyOwner
    - [Int] _transferOwnership

Contract functions details

+[Int] IBEPMint20 (IBEP20)
    -[Ext] farm

+[Int] IBurnERC20 (IBEP20)
    -[Ext] burnFrom

+ BEP20BUCCANEER (Context, IBurnERC20, IBEPMint20, Ownable)
    <Constructor>
    -[Pub] setNFTCenter
    -[Ext] getOwner
    -[Ext] decimals
    -[Ext] symbol
    -[Ext] name
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom
    -[Pub] increaseAllowance
    -[Pub] decreaseAllowance
    -[Pub] farm
        -Modifier: onlyOwner
    -[Pub] burn
    -[Int] _transfer
    -[Int] _mint
    -[Int] _burn
    -[Int] _approve
    -[Int] _burnFrom
    -[Pub] burnFrom

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Low issue
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

- **Critical Severity Issues**
  No critical severity issue found.
- **High Severity Issues**
  No high severity issue found.
- **Medium Severity Issues**
  No Medium severity issue found.
- **Low Severity Issues**
  One low severity issue found.

1. Unlocked Compiler Version.

- **Description**

  The _msgData, _mod function does nothing.
  The getOwner and Owner functions returns the same value.

- **Location**

  123, 258, 273

- **Recommendation**

  We advise to remove unused code.
  We advise to remove getOwner function.

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- Buccaneer Contract:
    - Owner can change ownership.
    - Owner can renounce ownership.
    - Owner can mint maximum 1000000000 tokens.
    - _nftManager can burn allowed tokens.
    - Developer address can change _nftManager address. (_dev address is define at deployment time.)

Conclusion

Smart contract contains low severity issues!

HackSafe 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.