HackSafe

Smart Contract Security Audit Report

InfinityToken

April **2022**

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
InfinityToken

Deployer address
0xf05a8Cc47872B5C1De23bd2023C59cCdcDF90960

Client contacts
InfinityToken team

Blockchain
Binance smart chain

Website
Not provided by InfinityToken team.

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 InfinityToken Coin to perform an audit of smart contracts:

- https://bscscan.com/address/0x52E4339B4b9fF254738D6E971E83440F60DC029c#code

Contract Details

Token contract details for 21.04.2022

Contract name	: InfinityToken
Contract address	: 0x52E4339B4b9fF254738D6E971E83440F60DC029c
Total supply	: 99,549,537.623913
Token Ticker	: INF
Decimals	: 18
Token Holders	: 971
Transactions count	: 5,312
Contract deployer address	: 0xf05a8Cc47872B5C1De23bd2023C59cCdcDF90960

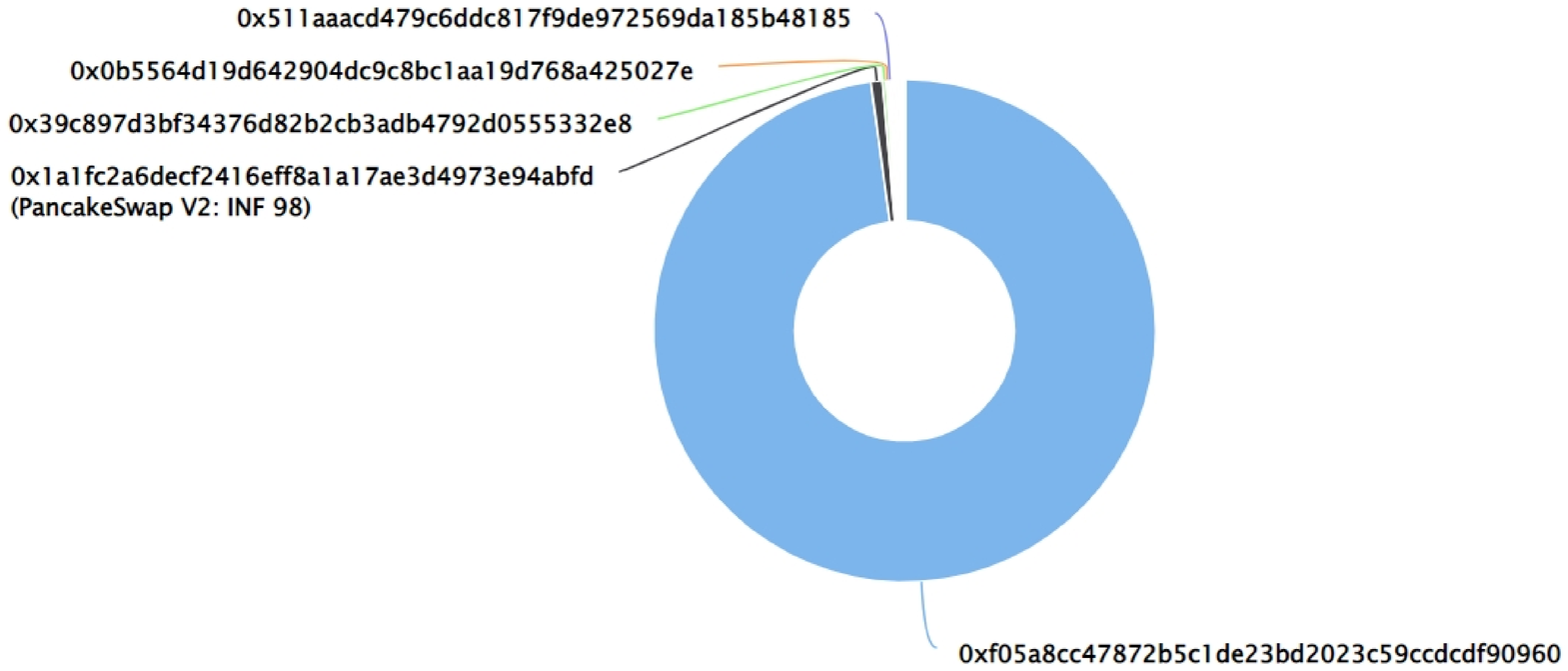
InfinityToken Token Distribution

The top 500 holders collectively own 99.99% (99,543,944.81 Tokens) of InfinityToken

Token Total Supply: 99,549,537.62 Token | Total Token Holders: 971

InfinityToken Top 500 Token Holders

Source: BscScan.com



InfinityToken Top 10 Token Holders

(A total of 99,103,398.34 tokens held by the top 10 accounts from the total supply of 99,549,537.62 token)

Rank	Address	Quantity (Token)	Percentage
1	0xf05a8cc47872b5c1de23bd2023c59ccdcdf90960	97,424,700.175669219308604715	97.8655%
2	PancakeSwap V2: INF 98	729,243.760557258193456642	0.7325%
3	0x39c897d3bf34376d82b2cb3adb4792d0555332e8	229,239.477001460469497994	0.2303%
4	0x0b5564d19d642904dc9c8bc1aa19d768a425027e	168,096.768570351524015088	0.1689%
5	0x511aaacd479c6ddc817f9de972569da185b48185	145,766.895618627617840141	0.1464%
6	0x2ac90a3cf91bee005c45e3c2ca58e93c2da07082	118,192.63173261148153947	0.1187%
7	0x998812f5f4659addc241c38657145e8f5af72553	83,794.494933200760084872	0.0842%
8	0x708352d6a248bbe750698ccf8c60dfb82bdeac1f	71,172.961605826987036971	0.0715%
9	0xb21b2c0261c595780cc9b28ebcf11adb845e416f	70,901.696571672595230526	0.0712%
10	0x075bf7a941a9b43dde4749b43cf909d608d7ffc0	62,289.473864518146588657	0.0626%

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 #

+ IBEPMint20 (IBEP20)
    -[Ext] mint #

+ Context
    -[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 #
      -modifiers: onlyOwner
    -[Pub] transferOwnership #
      -modifiers: onlyOwner
    -[Int] _transferOwnership #

Contract functions details

+ BEP20InfinityToken (Context, IBEPMint20, Ownable)
    - <constructor> #
    -[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] mint #
      -modifiers: onlyOwner
    -[Pub] burn #
      -[Pub] setBot #
        -modifiers: onlyOwner
      -[Int] _transfer #
      -[Int] _mint #
      -[Int] _burn #
      -[Int] _approve #
      -[Int] _burnFrom

($) = payable function
= non-constant function

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 issues found.

Low Severity Issues

One low severity issue found.

1. Scoping and Declarations.

Unused function.

- **Description**

  The mul, mod, mod, div, div, _msgData functions do nothing.

- **Location**

  mul, mod, mod, div, div, _msgData function.

- **Recommendation**

  We advise to remove unused code which can help you to develop clean coding style and save some computational gas too.

Owner Privileges

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

- InfinityToken Contract:
    - Owner can transfer ownership.
    - Owner can renounce ownership.
    - Owner can mint maximum 100000000 tokens.
    - Owner can set bot.

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

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.