HackSafe

Smart Contract Security Audit Report

TOTOZ

May 2022

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
TOTOZ

Deployer address
0x17Ab3461a1290515b865111fb40c02e9Fd0e86C2

Client contacts
TOTOZ team

Blockchain
Binance Smart Chain

Website
Not provided by TOTOZ 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

HackSafe was commissioned by TOTOZ to perform an audit of smart contracts:

- https://bscscan.com/address/0x69798b3a45a7bb93c825c56835ec84087d78781b#code

Contract Details

Token contract details for 13.05.2022

Contract name	: Totoz
Contract address	: 0x69798B3A45a7bB93C825C56835ec84087D78781b
Total supply	: 8,000,000,000,000,000
Token Ticker	: TOTOZ
Decimals	: 15
Token Holders	: 216 address
Transactions count	: 301
Contract deployer address	: 0x17Ab3461a1290515b865111fb40c02e9Fd0e86C2

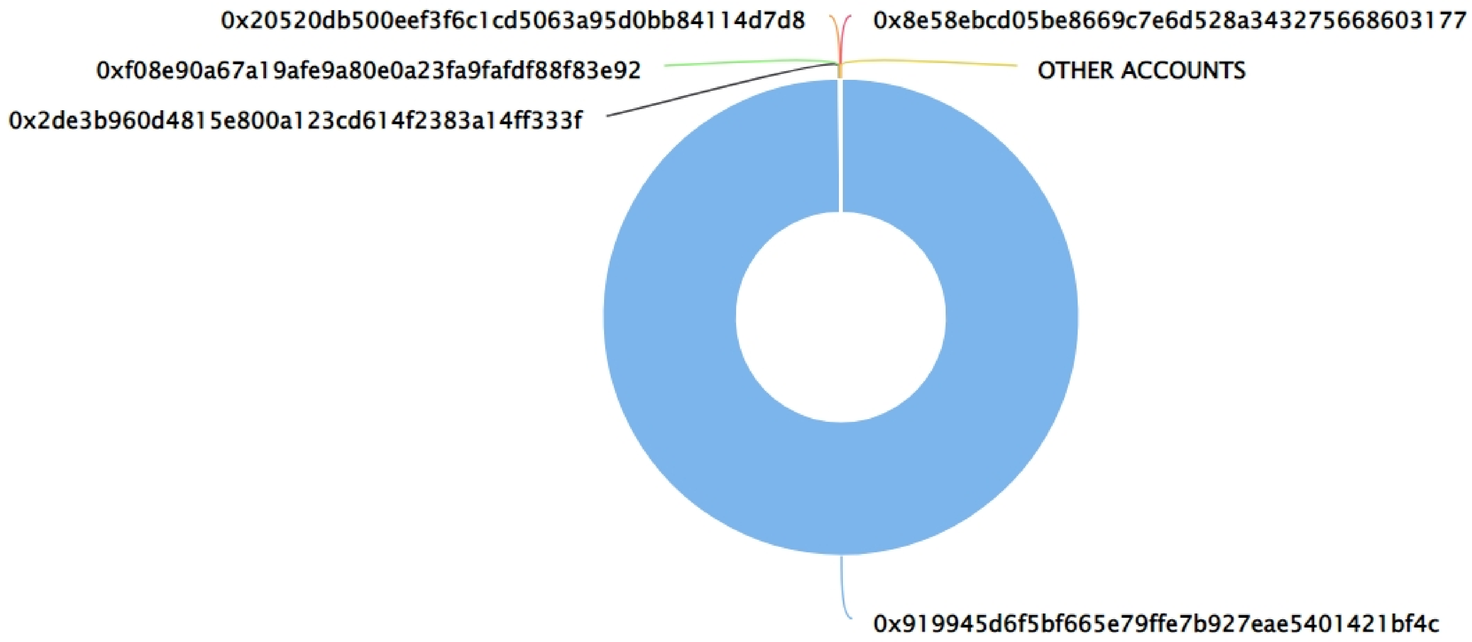
TOTOZ Token Distribution

The top 500 holders collectively own 100.00% (8,000,000,000,000,000.00 Tokens) of TOTOZ

Token Total Supply: 8,000,000,000,000,000.00 Token | Total Token Holders: 216

TOTOZ Top 500 Token Holders

Source: BscScan.com



TOTOZ Top 20 Token Holders

(A total of 8,000,000,000,000,000.00 tokens held by the top 500 accounts from the total supply of 8,000,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x919945d6f5bf665e79ffe7b927eae5401421bf4c	7,991,811,688,923,060.7	99.8976%
2	0x2de3b960d4815e800a123cd614f2383a14ff333f	918,849,000,000	0.0115%
3	0xf08e90a67a19afe9a80e0a23fa9fafdf88f83e92	787,500,000,000	0.0098%
4	0x20520db500eef3f6c1cd5063a95d0bb84114d7d8	750,000,000,000	0.0094%
5	0x7ea5bf8f97606980a17986819bfd78ba990d88ab	609,386,250,000	0.0076%
6	0x5653fe090baaa7a9a786109df8a9b60649e31d1f	455,884,500,000	0.0057%
7	0xeff1420cba5b37665185e66ff1a1ebd1af67fe67	416,110,000,000	0.0052%
8	0xb3163941b2e08e8e21f23fdfc7d8df9c7dc8b149	400,000,000,000	0.0050%
9	0x2aac5b1e34ba3f45a730ee724b8a45b8fedd0c63	382,500,000,000	0.0048%
10	0xfaeed62c80ea583596ca229e6e04208b5483ea00	376,204,350,000	0.0047%
11	0x4cf07069215a27bdc64db7b415c7ff968ad1b187	375,760,000,000	0.0047%
12	0x156a3673e61a34cd6445741f33c2a93dfbed1e3d	279,880,000,000	0.0035%
13	0x7854151ae03d6bc512a2822852a153d32150be0b	244,662,500,000	0.0031%
14	0x08ddabbb6ad49bb8703258d39f69ecb4cf7f77ec	225,015,000,000	0.0028%
15	0xccc4c2f9d722ac21ce47ffab7e7efd8a1794d9a3	150,000,000,000	0.0019%
16	0x233e2bc1d0d4b29d9e25acf26dda24acb31eea78	147,200,000,000	0.0018%
17	0x3045a9fc4bf884fd127ea1cfc14992c1dc76a333	143,760,000,000	0.0018%
18	0x4bd0fec25d1dc4ce4bbb0d337754a7a9a428eebb	143,750,000,000	0.0018%
19	0x8a7a39399e2cb2319bf83bec4cab14d13d9eb0f5	75,000,000,000	0.0009%
20	0xaa01f1f58b243ccd8a52246f7c45be8b904de5f6	75,000,000,000	0.0009%

Contract functions details

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

+ [Int] IBEP20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

+ [Int] IBEP20Metadata (IBEP20)
    -[Ext] name
    -[Ext] symbol
    -[Ext] decimals

+ BEP20 (Context, IBEP20, IBEP20Metadata)
    -<constructor>
    - [Pub] name
    - [Pub] symbol
    - [Pub] decimals
    - [Pub] totalSupply
    - [Pub] balanceOf
    - [Pub] transfer #
    - [Pub] allowance
    - [Pub] approve #
    - [Pub] transferOwnership#
      -modifiers: onlyOwner
    - [Pub] transferFrom #
    - [Int] _transfer #
    - [Int] _mint #
    - [Int] _approve #
    - [Int] _spendAllowance #
    - [Int] _beforeTokenTransfer #
    - [Int] _afterTokenTransfer #

Contract functions details

+ Totoz (BEP20)
    -< constructor > #

($) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
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.	Passed
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. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version v0.8.0 the contract should contain the following line:

  pragma solidity 0.8.0;

Owner Privileges

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

- TOTOZ Contract:
    - Owner can transfer ownership.

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.