HackSafe

Smart Contract Security Audit Report

Titan War

April **2022**

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
Titan War

Deployer address
0x70224d8813ba9e5c85fefb4d0a68344405fe0746

Client contacts
Titan War team

Blockchain
Binance smart chain

Website
https://titanwar.io/

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 Titan War to perform an audit of smart contracts:

- https://bscscan.com/address/0x76F34cd142ca4a5ea2E197ebffbF5234A1c29268#code

Contract Details

Token contract details for 16.04.2022

Contract name	: Titan War
Contract address	: 0x76F34cd142ca4a5ea2E197ebffbF5234A1c29268
Total supply	: 600, 000, 000
Token Ticker	: TITAN
Decimals	: 8
Token Holders	: 10,524
Transactions count	: 28,971
Contract deployer address	: 0x70224d8813ba9e5c85FEfb4d0a68344405FE0746

Titan War Token Distribution

Titan War Top 10 Token Holders

Rank	Address	Quantity	Percentage	Value
1	0x4eec73a7d6b3ed5359bc08f831c4f7cf21e63f07	10,000,000,000,000,000,000,000,000,000,000,000.23857981	1,666,666,666,666,670,000,000,000,000.0000%	$183,000,000,000,000,000,000,000,000,000.00
2	Hotbit 2	44,531,577,674.30101716	7,421.9296%	$814.93
3	PancakeSwap V2: TITAN 70	1,191,172,950.73954421	198.5288%	$21.80
4	0xccd09e3393a64ba783327001338ce2b914a2d6d1	874,775,171	145.7959%	$16.01
5	0x2dbfafc41d97a70ee52f2262beeeeaa31b22f6a2	733,747,609	122.2913%	$13.43
6	0xa750798ca92127025e174ccaeb5514aa8a6ec9ea	715,701,951	119.2837%	$13.10
7	0x62a61618d0d61c281fadcd1b3dec45b49bd6a124	648,736,668.30329609	108.1228%	$11.87
8	0x1feb4932b8e0d53a495d5ed46234df0b7e8cb1aa	591,403,475.14614597	98.5672%	$10.82
9	0x7946bba50cf7ad3ca890be51405f5bf6dbd2f7ae	418,893,955	69.8157%	$7.67
10	0x0298afb0fbdcf298d4b4ee0806719b5f9d1b7630	336,297,275	56.0495%	$6.15

Contract functions details

+ [Int] IERC20
    - [Ext] totalSupply
    - [Ext] balanceOf
    - [Ext] allowance
    - [Ext] transfer #
    - [Ext] approve #
    - [Ext] transferFrom #

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

ForeignToken
    - [Pub] balanceOf
    - [Pub] transfer #

+ BEP20Basic
    - [Pub] balanceOf
    - [Pub] transfer #

+ BEP20 (BEP20Basic)
    - [Pub] allowance
    - [Pub] transferFrom #
    - [Pub] approve #

+ TitanWar (BEP20)
    - [Pub] <Constructor>#
    - [Ext] setTaxFeePercent #
      - modifiers: onlyOwner
    - [Pvt] calculateTaxFee
    - [Pvt] removeAllFee #
    - [Pvt] restoreAllFee #
    - [Ext] setLiquidityFeePercent #
      - modifiers: onlyOwner

Contract functions details

- [Pvt] calculateLiquidityFee
- [Pub] transferOwnership #
  - modifiers: onlyOwner
- [Pub] finishDistribution #
  - modifiers: onlyOwner,canDistr
- [Pvt] distr #
  - modifiers: canDistr
- [Pub] totalFees
- [Int] Distribute #
  - modifiers: onlyOwner
- [Ext] DistributeAirdrop #
  - modifiers: onlyOwner
- [Ext] DistributeAirdropMultiple #
  - modifiers: onlyOwner
- [Pub] updateTokensPerEth #
  - modifiers: onlyOwner
- [Ext] ($)
- [Pub] getTokens ($)
  - modifiers: canDistr
- [Pub] balanceOf
- [Pub] transfer #
  - modifiers: onlyPayloadSize
- [Pub] transferFrom #
  - modifiers: onlyPayloadSize
- [Pub] approve #
- [Pub] allowance
- [Pub] getTokenBalance
- [Pub] withdrawAll #
  - modifiers: onlyOwner
- [Pub] withdraw #
  - modifiers: onlyOwner
- [Pub] burn #
  - modifiers: onlyOwner
- [Pub] withdrawForeignTokens #
  - modifiers: onlyOwner

($) = 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.	Low issue
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.	Medium issue
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

Two medium severity issues found.

1. Wrong total supply restriction

- **Description:**

  The function Distribute() checks that totalDistributed < totalSupply, but should check totalDistributed + _amount < totalSupply.

- **Recommendation:**

  We advise to check that the result will not exceed totalSupply.

2. getTokens function errors

- **Description:**

  bonusCond1 = bonusCond2 = bonusCond3, so all the conditions will not work as expected.

- **Recommendation:**

  We advise you to recheck logic of this part of the contract.

Low Severity Issues

No low severity issues 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.

Security Issues

- **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 v0.4.26 the contract should contain the following line:

  pragma solidity 0.4.26;

2. Out of gas

- **Description**

  The function DistributeAirdropMultiple() uses the loop for distributing tokens as airdrop.

- **Recommendation**

  We advise to check that the addresses array length is not too big.

Owner Privileges

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

- Titan War Contract:
    - Owner can burn.
    - Owner can withdraw BNBs from the contract.
    - Owner can withdraw tokens from contract.
    - Owner can stop distribution.
    - Owner can distribute tokens.
    - Owner can change tokensPerEth value.

Conclusion

Smart contract contains low and medium 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.