



Smart Contract Security Audit Report

Titania Token

December 2022

Security Status



www.hacksafe.io

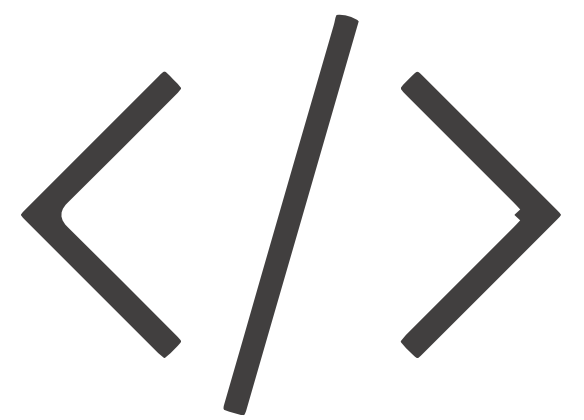


Audit Details



Audited project

Titania Token



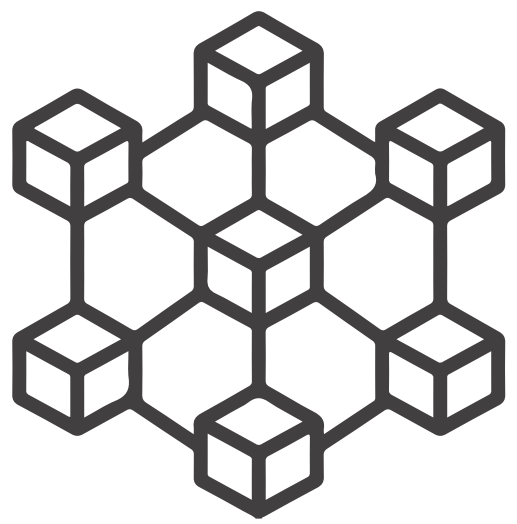
Deployer address

0x47398d43f01a2a1c4ce272f4dc6ac3c2156e4b70



Client contacts

Titania Token Team



Blockchain

Binance smart chain



Website

<https://titaniatoken.com/>

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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by Titania Token perform an audit of smart contracts:

- <https://bscscan.com/token/0x5108C0E857b30A8d191554134628fe0f1B7e78b4#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 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.

Contract Details

Token contract details for 08.12.2022

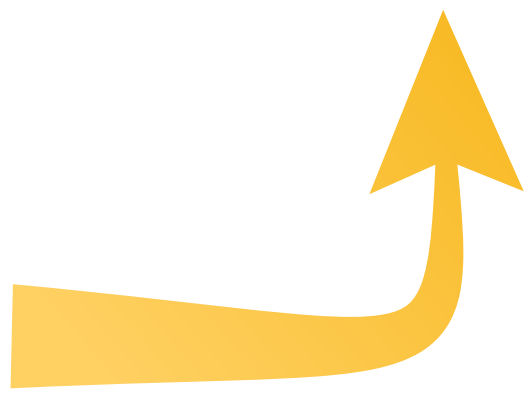
Token Type	: DEFI
Contract name	: TITANIA
Contract address	: 0x5108C0E857b30A8d191554134628fe0f1B7e78b4
Total supply	: 91,395,256,665,687,500.438732
Token ticker	: TITANIA
Decimals	: 9
Token Holders	: 8,005
Transactions count	: 79,666
Compiler version	: v0.8.2+commit.661d1103
Contract deployer address	: 0x47398d43f01a2a1c4ce272f4dc6ac3c2156e4b70
Owner address	: 0x00

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Secure”**. This token contract does not contain owner control as ownership has been renounced, which do make it fully decentralized as owner does not have control over smart contract.

Insecure	Poor secured	Secure	Well-secured
----------	--------------	--------	--------------

You are here



We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 1 low.

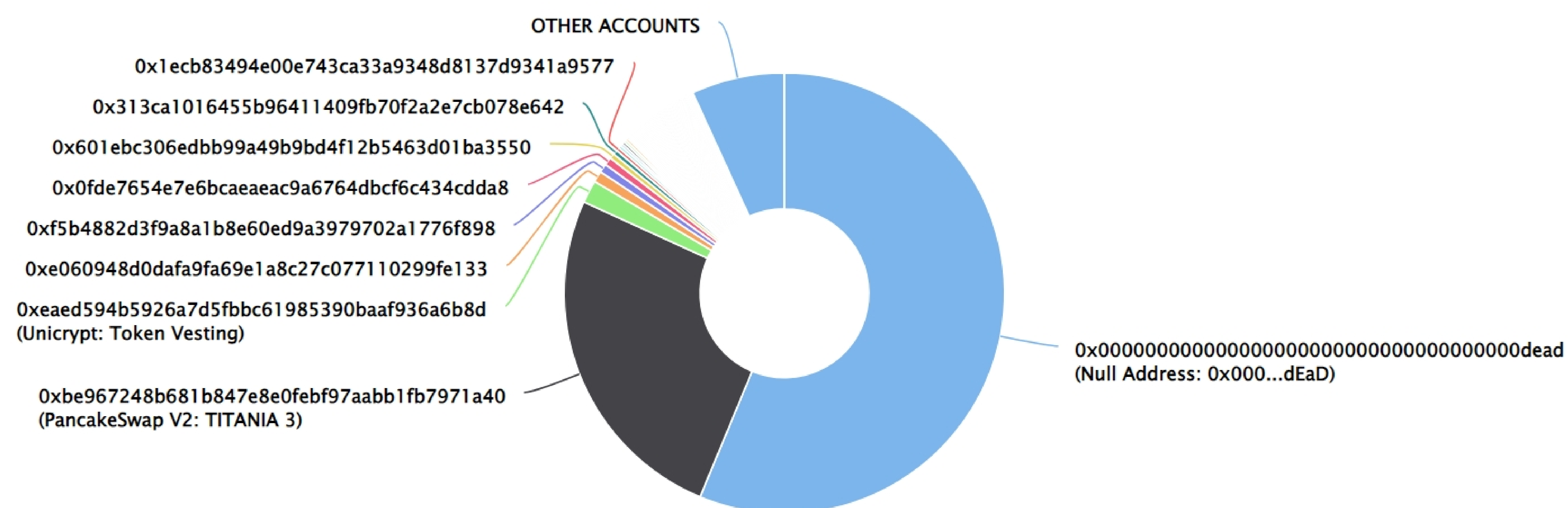
Titania Token Distribution

💡 The top 100 holders collectively own 93.19% (85,168,578,479,964,600.00 Tokens) of Titania Token


💡 Token Total Supply: 91,395,256,665,687,500.44 Token | Total Token Holders: 8,005

Titania Token Top 100 Token Holders

Source: BscScan.com

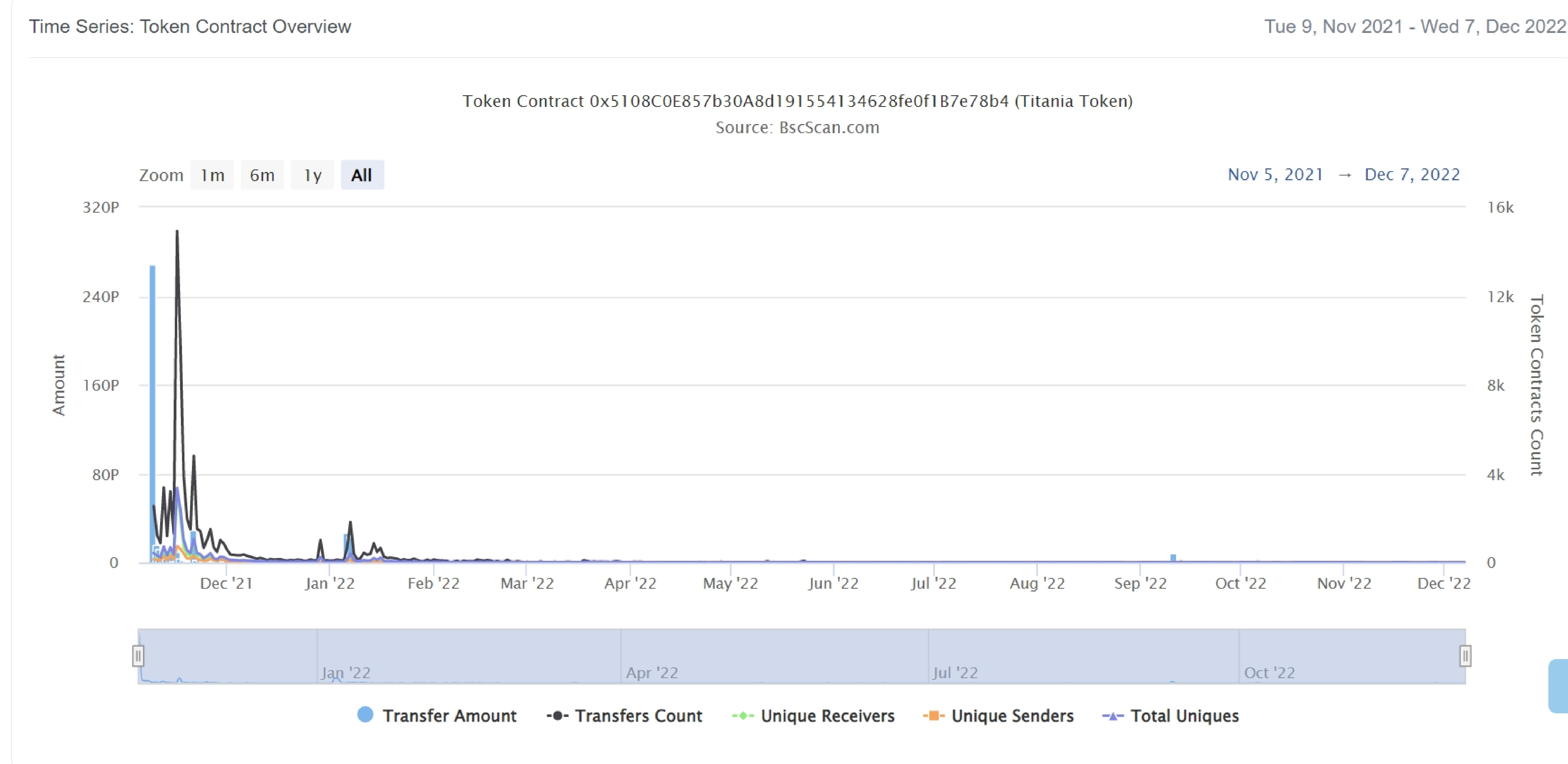


Titania Token Top 20 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	51,416,087,507,893,900.773472169	56.2568%
2	PancakeSwap V2: TITANIA 3	23,343,112,697,522,000.498950378	25.5408%
3	 Unicrypt: Token Vesting	1,531,917,583,664,300.5904703	1.6761%
4	0xe060948d0dafa9fa69e1a8c27c077110299fe133	743,491,552,698,963.744886486	0.8135%
5	0xf5b4882d3f9a8a1b8e60ed9a3979702a1776f898	578,345,531,977,105.099998493	0.6328%
6	0x0fde7654e7e6bcaeaeac9a6764dbcf6c434cdda8	544,625,270,194,658.426808122	0.5959%
7	0x601ebc306edbb99a49b9bd4f12b5463d01ba3550	350,976,275,114,025.270513435	0.3840%
8	0x313ca1016455b96411409fb70f2a2e7cb078e642	292,723,585,800,032.369462396	0.3203%
9	0x1ecb83494e00e743ca33a9348d8137d9341a9577	232,159,950,012,986.167446967	0.2540%
10	0xb03025b8cefb37fcb7161561f7456bff6766a3b8	190,282,150,801,293.576149098	0.2082%
11	0xd5927a8a6215f5f5ee762c8bed136eb933384f5c	170,457,157,960,110.227945534	0.1865%
12	0xec6042cfb43c7ff768bf5ac0df56a5008ccc7787	161,309,008,732,210.704253059	0.1765%
13	0x65eace08f258639d997ac8bbd49b2622c5a72d4e	157,983,038,739,302.277635574	0.1729%
14	0x5e703467c607c94ab2d24e9b4ebdc6fe8977adb1	156,261,722,508,895.793108382	0.1710%
15	0x7899268dc93ecbaf5ae4d34282509afe7f159f33	132,913,342,416,570.903425826	0.1454%
16	0x86869bb5d669bc0fc7c94fe03b723048cb5b95c6	130,144,489,793,096.019999897	0.1424%
17	0x6323760da7283764df02fb0f16823e46006c9308	128,423,213,696,682.208172322	0.1405%
18	0xcff31d815daebd43c509129effee754a619e9e7f	123,658,835,552,089.229357744	0.1353%
19	0xd055da76fa4499a35a5e2851d63668f469ff8605	115,939,351,251,642.105882233	0.1269%
20	0x403c26d8457b809f1778a4209cfd565831efe63d	111,128,755,532,626.251326454	0.1216%

Titania Token Distribution

Titania Token Contract Overview



Contract functions details

+Context

- [Int] _msgSender
- [Int] _msgData

+ [Int] IBEP20

- [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
- [Pvt] _functionCallWithValue

+Ownable (Context)

- [Pub] owner
- [Pub] renounceOwnership #
-modifiers: onlyOwner
- [Pub] transferOwnership #
-modifiers: onlyOwner

+TITANIA (Context, IBEP20, Ownable)

- <constructor> \$
- [Pub] name

Contract functions details

- [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] totalBurn
- [Pub] totalCharity
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
 - modifiers: onlyOwner
- [Ext] includeAccount #
 - modifiers: onlyOwner
- [Ext] setAsCharityAccount #
 - modifiers: onlyOwner
- [Pub] updateFee #
 - modifiers: onlyOwner
- [Pvt] _approve #
- [Pvt] _transfer #
- [Pvt] _transferStandard #
- [Pvt] _standardTransferContent #
- [Pvt] _transferToExcluded #
- [Pvt] _excludedFromTransferContent #
- [Pvt] _transferFromExcluded #
- [Pvt] _excludedToTransferContent #
- [Pvt] _transferBothExcluded #
- [Pvt] _bothTransferContent #
- [Pvt] _reflectFee #
- [Pvt] _getValues
- [Pvt] _getTBasics

Contract functions details

- [Pvt] getTTransferAmount
- [Pvt] _getRBasics
- [Pvt] _getRTransferAmount
- [Pvt] _getRate
- [Pvt] _getCurrentSupply
- [Pvt] _sendToCharity #
- [Pvt] removeAllFee #
- [Pvt] restoreAllFee #
- [Pvt] _getTaxFee

(\$) = 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
20.	Too old version	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 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 ^0.8.2 the contract should contain the following line:

```
pragma solidity 0.8.2;
```

Owner privileges :

- Titania Token Contract:
 - Owner can transfer/renounce ownership.
 - Owner can exclude/include accounts.
 - Owner can set as charity account.
 - Owner can update fee.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble, as smart contract ownership has not been renounced.

- transferOwnership
- renounceOwnership
- excludeAccount
- includeAccount
- setasCharityAccount
- updateFee

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.