TechRate
April, 2022

SMART CONTRACTS SECURITY AUDIT REPORT

Audit Details

Audited project

Cactus

Deployer address

0xc08969b99547cb5f83a462acdaefc5f577ec7676

Client contacts:

Cactus team

Blockchain

Binance Smart Chain

Project website:

https://cactusexchange.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) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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

TechRate was commissioned by Cactus to perform an audit of smart contracts:
https://bscscan.com/address/0x649a339B8FC3A8bA0A03255c00fDC5D969684074#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 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

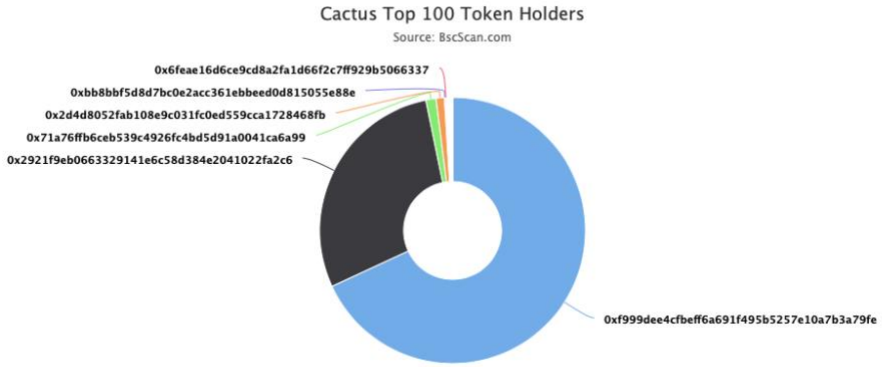
Token contract details for 29.04.2022

Contract name	Cactus
Contract address	0x649a339B8FC3A8bA0A03255c00fDC5D969684074
Total supply	19,353,067.2
Token ticker	CACTT
Decimals	18
Token holders	27
Transactions count	33
Top 100 holders dominance	100.00%
Total fees	1116000000000000000000
Liquidity fee	0
Tax fee	150
Liquidity address	0x649a339b8fc3a8ba0a03255c00fdc5d969684074
Contract deployer address	0xc08969b99547cb5f83a462acdaefc5f577ec7676
Owner address	0xf999dee4cfbeff6a691f495b5257e10a7b3a79fe

Cactus Token Distribution

The top 100 holders collectively own 100.00% (19,352,552.61 Tokens) of Cactus

Token Total Supply: 19,353,067.20 Token | Total Token Holders: 27

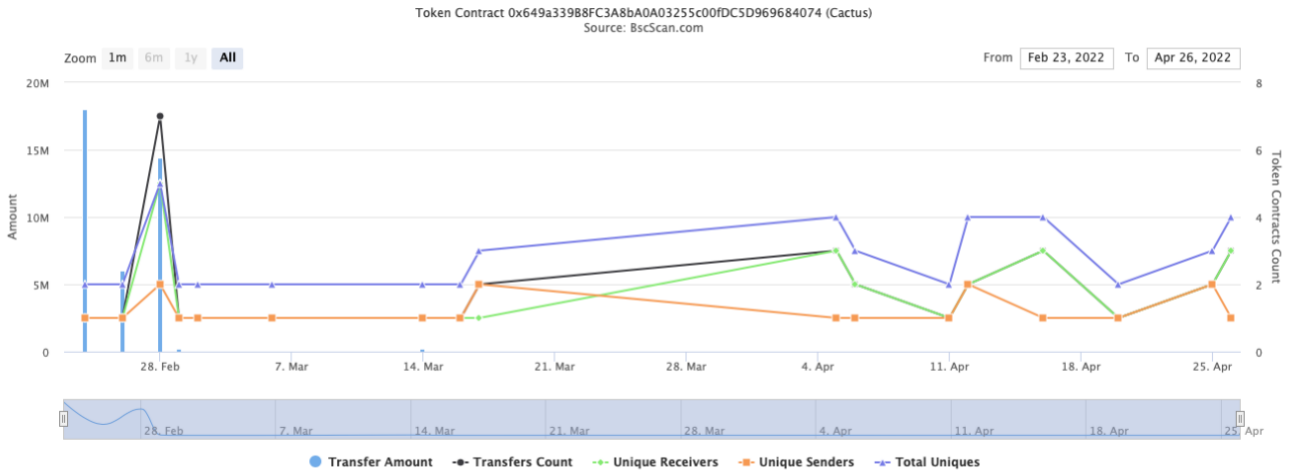


(A total of 19,352,552.61 tokens held by the top 100 accounts from the total supply of 19,353,067.20 token)

Cactus Contract Interaction Details

Time Series: Token Contract Overview

Thu 24, Feb 2022 - Tue 26, Apr 2022



Cactus Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xf999dee4cfbeff6a691f495b5257e10a7b3a79fe	13,181,824.315778886476627022	68.1123%
2	0x2921f9eb0663329141e6c58d384e2041022fa2c6	5,548,800	28.6714%
3	0x71a76ffb6ceb539c4926fc4bd5d91a0041ca6a99	240,000	1.2401%
4	0x2d4d8052fab108e9c031fc0ed559cca1728468fb	192,000	0.9921%
5	0xbb8bbf5d8d7bc0e2acc361ebbeed0d815055e88e	24,000	0.1240%
6	0x6feae16d6ce9cd8a2fa1d66f2c7ff929b5066337	19,152	0.0990%
7	0x4d7b615eff559dec8886263aaa48c66447a76eae	18,624.55817647565817912	0.0962%
8	0xd9e803d1c27d3b3a43f5b3f37d9ea16dda8089de	13,440	0.0694%
9	0xc2693671f55f84b26aa804430310bc2dc20d56b5	10,003.2	0.0517%
10	0x01b2e12c10f39e95ef38b99ca081891fa2c7a499	9,600.287719832813494392	0.0496%

Contract functions details

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Int] _transferOwnership #

+ Pausable (Context)
  - [Pub] <Constructor> #
  - [Pub] paused
  - [Int] _pause #
    - modifiers: whenNotPaused
  - [Int] _unpause #
    - modifiers: whenPaused

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

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #

- [Int] verifyCallResult

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ BaseToken (Pausable, Ownable)
  - [Pub] cap
  - [Pub] pause #
    - modifiers: onlyOperator
  - [Pub] unpause #
    - modifiers: onlyOperator
  - [Pub] updateOperator #
    - modifiers: onlyOperator
  - [Pub] setTreasuryAddress #
    - modifiers: onlyOperator,whenNotPaused
  - [Ext] getOwner

+ CactusToken (Context, IERC20, BaseToken, IERC20Metadata)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Int] _approve #
  - [Pub] transferFrom #

- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalFees
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] setTaxFeePercent #
  - modifiers: onlyOperator
- [Pub] setLiquidityFeePercent #
  - modifiers: onlyOperator
- [Pub] setMarketingFeePercent #
  - modifiers: onlyOperator
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOperator
- [Pub] includeInReward #
  - modifiers: onlyOperator
- [Prv] _transferBothExcluded #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _reflectFee #
- [Int] _transfer #
  - modifiers: whenNotPaused
- [Prv] _tokenTransfer #
- [Pub] burn #
  - modifiers: onlyOperator
- [Ext] mint #
  - modifiers: onlyOperator
- [Int] _mint #
- [Pub] excludeFromFee #
  - modifiers: onlyOperator
- [Pub] includeInFee #
  - modifiers: onlyOperator
- [Pub] isExcludedFromFee
- [Prv] _getTValues
- [Prv] _getValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Pub] transferLiquidityOwnership #
  - modifiers: onlyOperator
- [Prv] _takeMarketingFee #
- [Prv] calculateTaxFee

- [Prv] calculateLiquidityFee
- [Prv] calculateMarketingFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] setTeamAddress #
  - modifiers: onlyOperator

($) = payable function
= non-constant function

Issues Checking Status

	Issue description	Checking status
1.	**Compiler errors.**	Passed
2.	**Race conditions and Reentrancy. Cross-function race conditions.**	Passed
3.	**Possible delays in data delivery.**	Passed
4.	**Oracle calls.**	Passed
5.	**Front running.**	Passed
6.	**Timestamp dependence.**	Passed
7.	**Integer Overflow and Underflow.**	Passed
8.	**DoS with Revert.**	Passed
9.	**DoS with block gas limit.**	Low issues
10.	**Methods execution permissions.**	Passed
11.	**Economy model of the contract.**	Passed
12.	**The impact of the exchange rate on the logic.**	Passed
13.	**Private user data leaks.**	Passed
14.	**Malicious Event log.**	Passed
15.	**Scoping and Declarations.**	Passed
16.	**Uninitialized storage pointers.**	Passed
17.	**Arithmetic accuracy.**	Passed
18.	**Design Logic.**	High issue
19.	**Cross-function race conditions.**	Passed
20.	**Safe Open Zeppelin contracts implementation and usage.**	Passed
21.	**Fallback function security.**	Passed

Security Issues

High Severity Issues

1. Abuse of authority

Issue:

- The function `burn()` could be called only by the operator and gives him ability to burn tokens from any address.

Recommendation:
Do not allow anybody to touch users' balances.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

2. Out of gas

Issue:

- The function `includeInReward()` uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.
- The function `_getCurrentSupply()` also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

Recommendation:
Check that the excluded array length is not too big.

Owner privileges (In the period when the owner is not renounced)

- Operator can pause/unpause the contract.
- Operator can add operators addresses.
- Operator can change treasuryContract, liquidity and team addresses.
- Operator can change tax, marketing and liquidity fees.
- Operator can mint tokens according to cap value.
- Operator can exclude addresses from fees.

Conclusion

Smart contracts contain high severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are NOT provided by the team.

TechRate 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.