HackSafe

Smart Contract Security Audit Report

cVToken

December 2022

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
cVToken

Deployer address
0x750aecab50afcc205f2a6e9718383ad162026cbc

Client contacts
cVToken Team

Blockchain
Ethereum

Website
https://www.carvertical.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 to cVToken perform an audit of smart contracts:

- https://etherscan.io/token/0x50bC2Ecc0bfDf566664004803 8C1ABA7B7525683#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 06.12.2022

Token Type	: DEFI
Contract name	: cVToken
Contract address	: 0x50bC2Ecc0bfDf566664004803 8C1ABA7B7525683
Total supply	: 9,895,342,499.252622438690110649
Token ticker	: cV
Decimals	: 18
Token Holders	: 13,233
Transactions count	: 21,160
Compiler version	: v0.6.12+commit.27d51765
Contract deployer address	: 0x750aecab50afcc205f2a6e9718383ad162026cbc
Owner address	: No owner

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Secure”.** This token contract does not contain owner control, 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, 1 medium and 2 low.

Social profiles

Github profile	: https://github.com/carVertical
Telegram profile	: https://t.me/carVerticalio
Coinmarket profile	: https://coinmarketcap.com/currencies/carvertical/
Coingecko profile	https://www.coingecko.com/en/coins/carvertical/

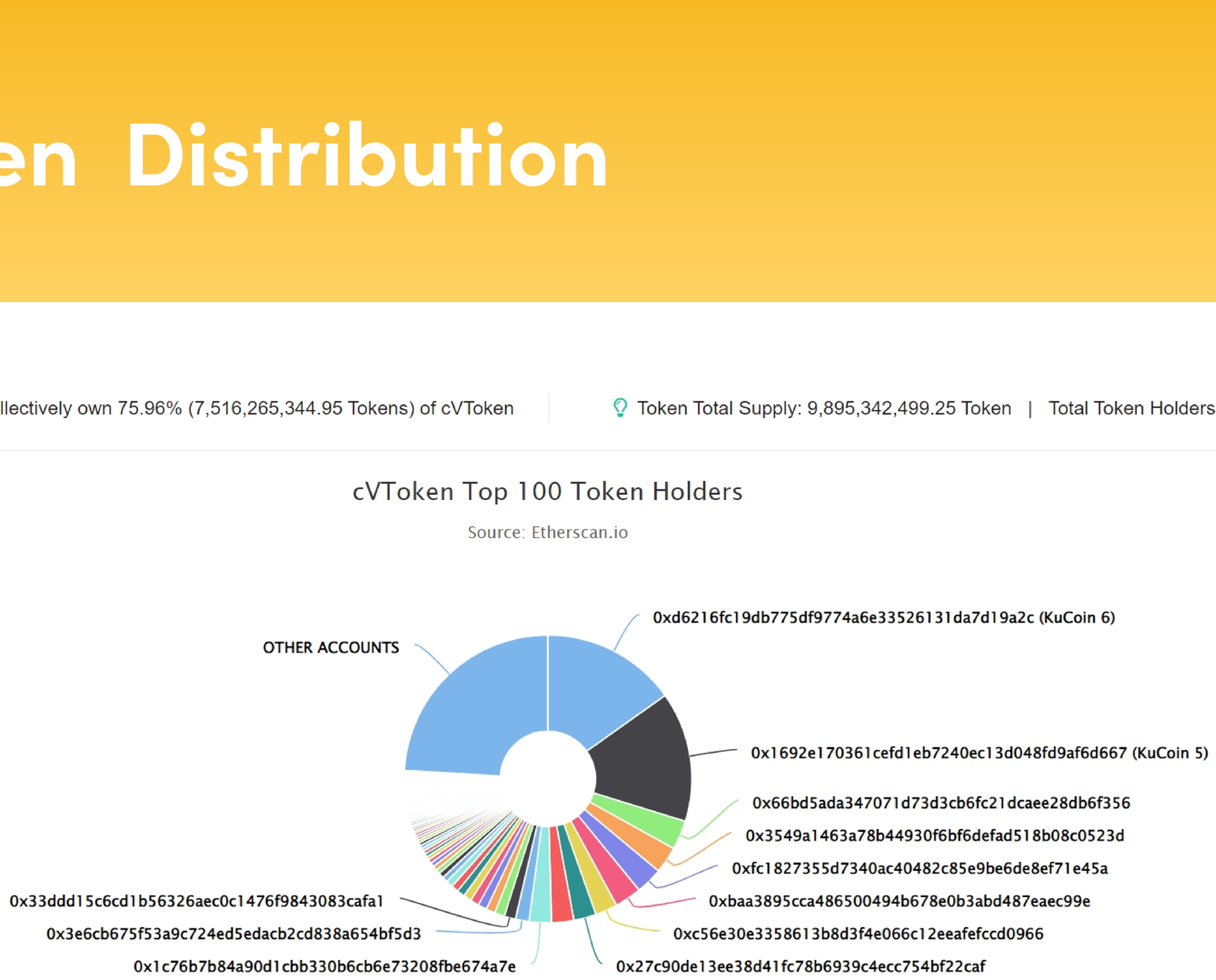
cVToken Distribution

The top 100 holders collectively own 75.96% (7,516,265,344.95 Tokens) of cVToken

Token Total Supply: 9,895,342,499.25 Token | Total Token Holders: 13,233

cVToken Top 100 Token Holders

Source: Etherscan.io



cVToken Top 20 Token Holders

(A total of 7,516,265,344.95 tokens held by the top 100 accounts from the total supply of 9,895,342,499.25 token)

Rank	Address	Quantity (Token)	Percentage
1	KuCoin 6	1,500,006,203.471119933395501132	15.1587%
2	KuCoin 5	1,446,885,276	14.6219%
3	0x66bd5ada347071d73d3cb6fc21dcaee28db6f356	323,349,744.1266	3.2677%
4	0x3549a1463a78b44930f6bf6defad518b08c0523d	297,934,319.34	3.0109%
5	0xfc1827355d7340ac40482c85e9be6de8ef71e45a	297,934,319.34	3.0109%
6	0xbaa3895cca486500494b678e0b3abd487eaec99e	297,934,319.34	3.0109%
7	0xc56e30e3358613b8d3f4e066c12eeafefccd0966	248,278,599.45	2.5090%
8	0x27c90de13ee38d41fc78b6939c4ecc754bf22caf	248,278,599.45	2.5090%
9	0x4c57513abec55c9fff8e7abf915b63e94edb0efc	248,278,599.45	2.5090%
10	0x1c76b7b84a90d1cbb330b6cb6e73208fbe674a7e	248,278,599.45	2.5090%
11	0x3e6cb675f53a9c724ed5edacb2cd838a654bf5d3	150,525,623.47824455999	1.5212%
12	0x33ddd15c6cd1b56326aec0c1476f9843083cafa1	124,986,947.185	1.2631%
13	0xb85aab871d5c2b9606b354381378a5288f365584	111,316,553.509366538936251332	1.1249%
14	0x5191465d5a1a2ee2b17eec35f1f70e5abfa47f2a	100,000,000.9999965	1.0106%
15	0x3fea3828f22d0ad4846f0d20cc145070d96bc85b	99,311,439.78	1.0036%
16	Null Address: 0x000...001	95,398,686.34069917	0.9641%
17	0x5839b48c154ebd48454153364b4ac512086cceb5	91,207,948.89254758	0.9217%
18	0x741fdcad2ca86545c9ecb0b085cb9950ea3d3abd	86,302,899.182688968058596303	0.8722%
19	0x7553289c4a4c52d377d24c212fabead93d0f7164	79,645,853.36743313	0.8049%
20	KuCoin 9	77,209,593.773359453970713464	0.7803%

cVToken Distribution

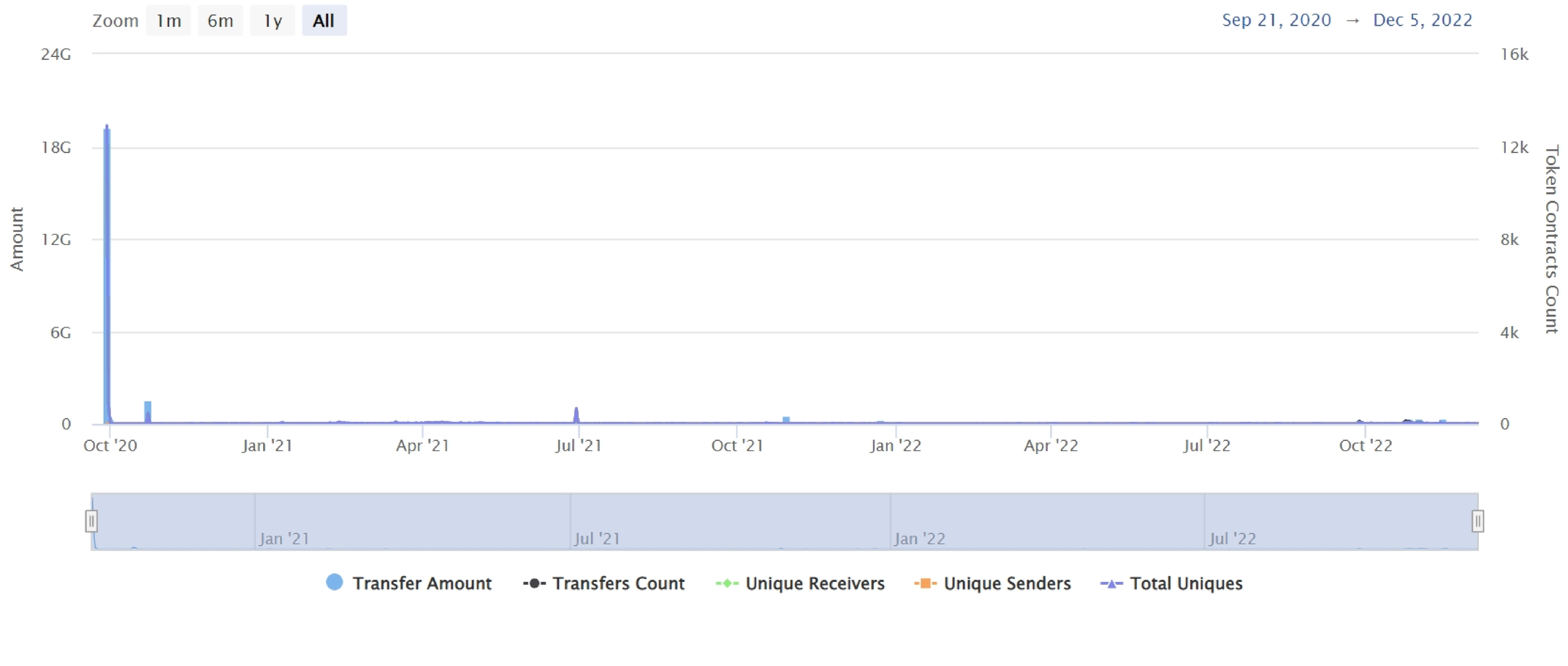
cVToken Overview

Time Series: Token Contract Overview

Tue 29, Sept 2020 - Mon 5, Dec 2022

Token Contract 0x50bC2Ecc0bfDf5666640048038C1ABA7B7525683 (cVToken)

Source: Etherscan.io



Contract functions details

+[Int] IERC20
    -[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

+cVToken (IERC20)
    -[Pub] <constructor>
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer #
    -[Pub] allowance
    -[Pub] approve #
    -[Pub] transferFrom #
    -[Pub] increaseAllowance #
    -[Pub] decreaseAllowance #
    -[Int] _transfer #
    -[Int] _burn #
    -[Int] _approve #
    -[Pub] burn #
    -[Ext] transferMany #
    -[Ext] permit #

Contract functions details

($) = 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.	Medium 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.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Low issue

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

One medium severity issue found.

1. Out of gas limit

- **Description**

  The function transferMany() uses the loop to transfer tokens from the _recipients list. Function will be aborted with OUT_OF_GAS exception if there will be a long recipients addresses list.

- **Recommendation**

  Use EnumerableSet instead of array or do not use long arrays.

Low Severity Issues

Two 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 di+erences in the generated bytecode between compilations due to di+ering compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be di-cult 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 ^0.6.12 the contract should contain the following line:

  pragma solidity 0.6.12;

2. Old compiler version

- **Description**

  Contract has been deployed using too old solidity version.

- **Recommendation**

  It is advisable to deploy contract using any of the latest version of solidity.

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.