HackSafe

Smart Contract Security Audit Report

CROWDHERO

December 2022

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
CROWDHERO

Deployer address
0x6f3580ecc71020c0bcdeaa7bc7a555d949697fef

Client contacts
CROWDHERO Team

Blockchain
Binance smart chain

Website
https://crowdhero.co/

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 CROWDHERO perform an audit of smart contracts:

- https://bscscan.com/token/0xcA76A652AC3c3F3b8669Bd41E22A9257bc6a6Bc6#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	: Token
Contract address	: 0xcA76A652AC3c3F3b8669Bd41E22A9257bc6a6Bc6
Total supply	: 1,000,000,000
Token ticker	: CRWD
Decimals	: 0
Token Holders	: 101
Transactions count	: 1,285
Compiler version	: v0.7.6+commit.7338295f
Contract deployer address	: 0x6f3580ecc71020c0bcdeaa7bc7a555d949697fef
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 1 low.

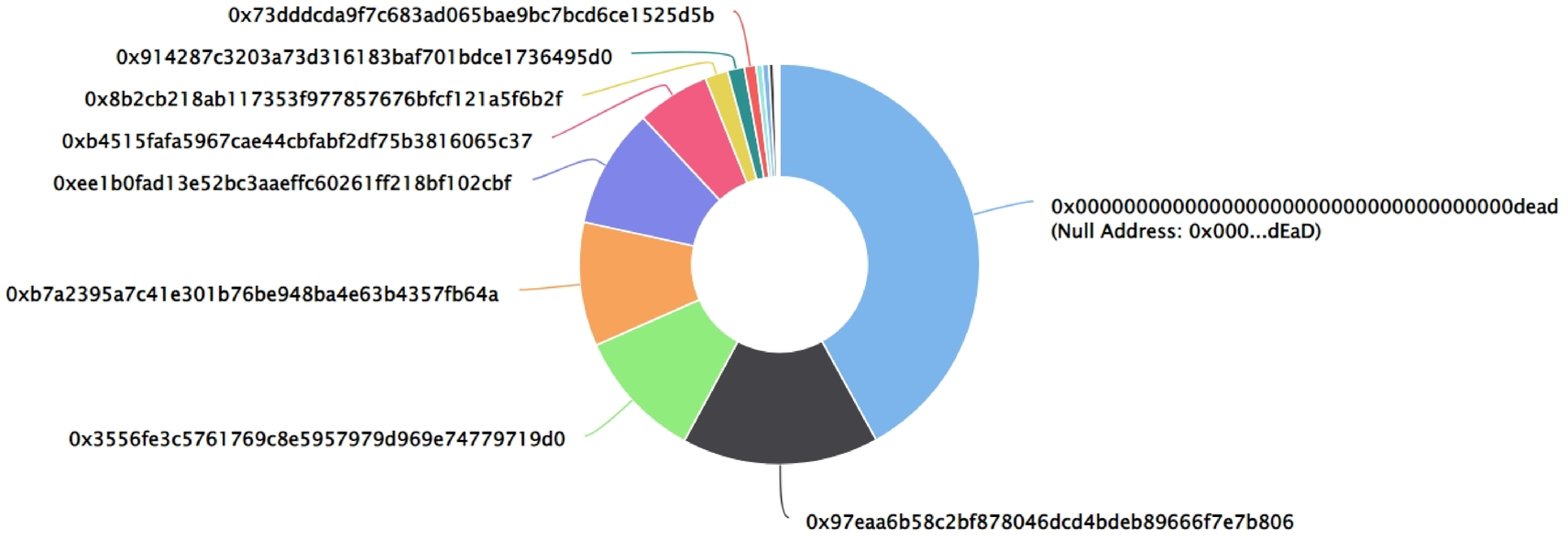
CROWDHERO Token Distribution

The top 100 holders collectively own 100.00% (999,999,999.00 Tokens) of CROWDHERO

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 101

CROWDHERO Top 100 Token Holders

Source: BscScan.com



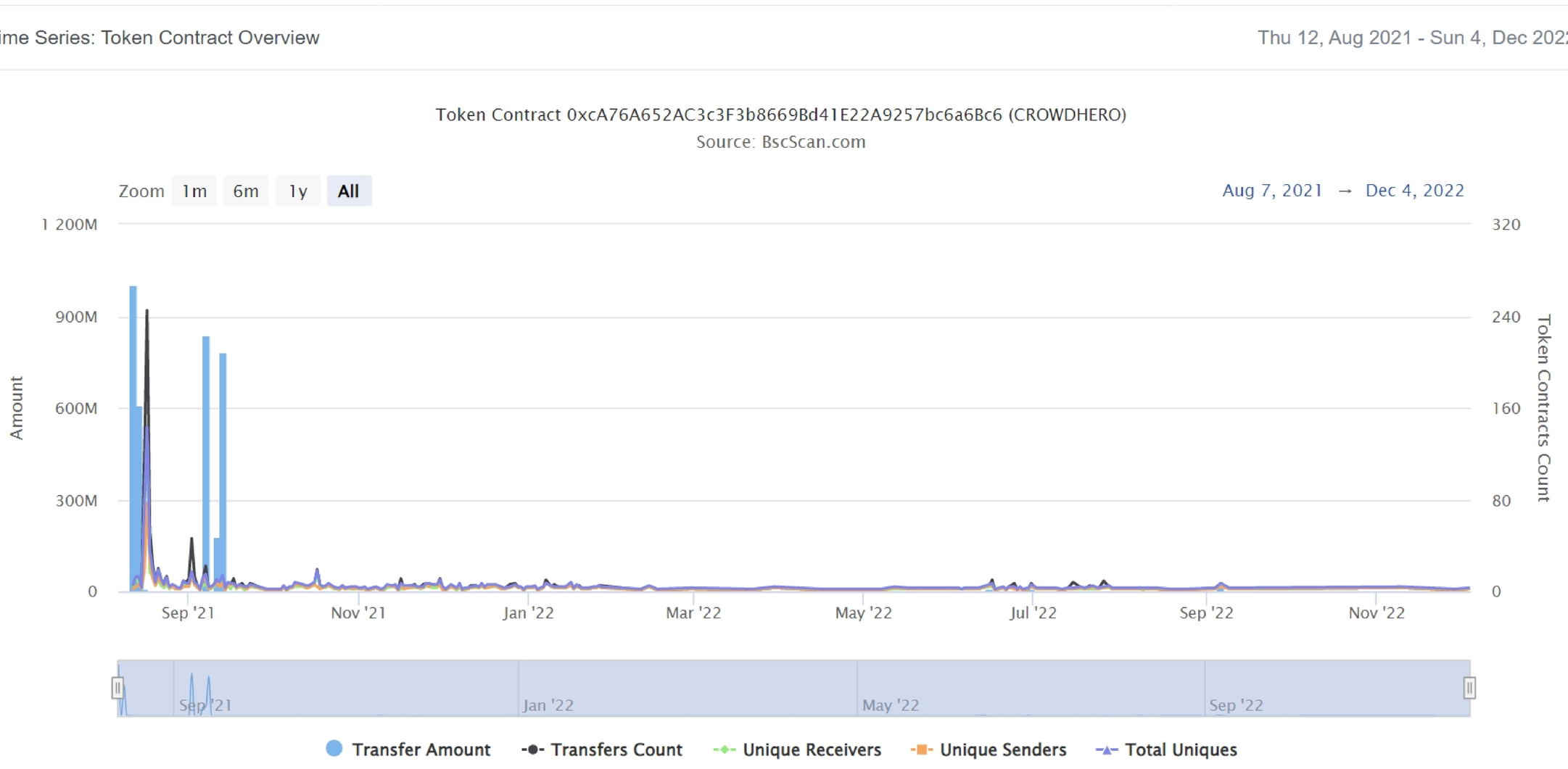
CROWDHERO Top 20 Token Holders

(A total of 999,999,999.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	420,000,005	42.0000%
2	0x97eaa6b58c2bf878046dcd4bdeb89666f7e7b806	159,000,000	15.9000%
3	0x3556fe3c5761769c8e5957979d969e74779719d0	105,000,000	10.5000%
4	0xb7a2395a7c41e301b76be948ba4e63b4357fb64a	100,000,000	10.0000%
5	0xee1b0fad13e52bc3aaeffc60261ff218bf102cbf	96,666,686	9.6667%
6	0xb4515fafa5967cae44cbfabf2df75b3816065c37	59,000,000	5.9000%
7	0x8b2cb218ab117353f977857676bfcf121a5f6b2f	18,600,000	1.8600%
8	0x914287c3203a73d316183baf701bdce1736495d0	13,491,468	1.3491%
9	0x73dddcda9f7c683ad065bae9bc7bcd6ce1525d5b	9,400,778	0.9401%
10	0x2fbdc7b4c37c65e79367445a3f66459af4c39898	5,327,048	0.5327%
11	0xe1eb5373e304fce1e6e23c5b05e4d08af9e7da15	5,000,100	0.5000%
12	0xbfcca5859055f39792fec5d8e5aa3e9f38f0052a	4,000,000	0.4000%
13	PancakeSwap V2: BSC-USD-CRWD	1,799,245	0.1799%
14	0xbde6e8309a72c239468b698a17c99a1b9a034ad0	1,307,544	0.1308%
15	0x179b3331dab65f4c23f124b550a22427b0f0acbd	221,442	0.0221%
16	0xca937139b2bf16cf158607c7a1a69e60bbd8282f	191,791	0.0192%
17	0x0474fc4e6969349595f6c09ec9a8f3e291348e1d	188,888	0.0189%
18	0xb0ab3f74ab1f70ae17f3432e2c9ab84fdd03eb75	181,818	0.0182%
19	0xec334f68e46f58d7c075440961ff79304ad728b7	150,000	0.0150%
20	0x872d233263d669c4630c363071545044cff3baa6	61,308	0.0061%

CROWDHERO Token Distribution

CROWDHERO Contract Overview



Contract functions details

+[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

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

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

+ERC20 (Context, IERC20)
    -<constructor>
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer #
    -[Pub] allowance
    -[Pub] approve #
    -[Pub] transferFrom #
    -[Pub] increaseAllowance #

Contract functions details

-[Pub] decreaseAllowance #
-[Int] _transfer #
-[Int] _mint #
-[Int] _burn #
-[Int] _approve #
-[Int] _setupDecimals #
-[Int] _beforeTokenTransfer

+Token (ERC20)
-<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.	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	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

One medium severity issue found.

1. Out of gas limit

- **Description**

  The constructor uses the loop to mint receivers_. Contract deployment will be aborted with OUT_OF_GAS exception if there will be a long receivers_ addresses list.

- **Recommendation**

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

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 ^0.8.0 the contract should contain the following line:

  pragma solidity 0.8.7;

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.