HackSafe

Smart Contract Security Audit Report

ASYAGRO

April **2022**

Security Status

★★★⯪☆

www.hacksafe.io

Audit Details

Audited project
ASYAGRO

Deployer address
0x8A9A638F389B22469D99CE156680822f53D77275

Client contacts
ASYAGRO team

Blockchain
Binance smartchain

Website
www.asyagro.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 ASYAGRO to perform an audit of smart contracts:

- https://bscscan.com/token/0xc0cc1e5761ba5786916fd055562551798e50d573

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issue 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

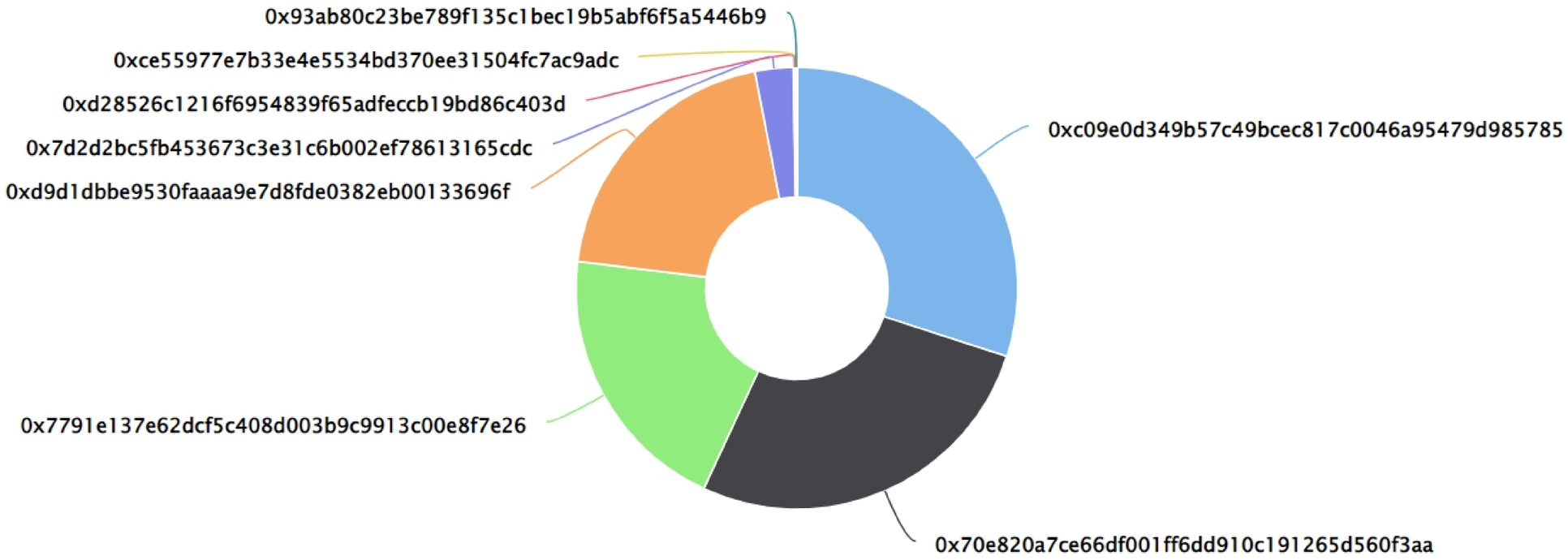
Token contract details for 08.04.2022

Contract name	: ASYAGRO
Contract address	: 0xC0Cc1e5761bA5786916FD055562551798E50d573
Total supply	: 7,500,000,000 (Max)
Token Ticker	: ASY
Decimals	: 18
Network	: Binance Smart Chain
Transactions count	: 203
Token Holders	: 159 addresses
Contract deployer address	: 0x8A9A638F389B22469D99CE156680822f53D77275
Owner address	: 0x70E820a7CE66Df001fF6DD910C191265D560f3aa

ASYAGRO Token Distribution

ASYAGRO Top 500 Token Holders

Source: BscScan.com



ASYAGRO Top 10 Token Holders

(A total of 7,498,029,150.81 tokens held by the top 10 accounts from the total supply of 7,500,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xc09e0d349b57c49bcec817c0046a95479d985785	2,250,000,000	30.0000%
2	0x70e820a7ce66df001ff6dd910c191265d560f3aa	2,021,186,418.833254296054594059	26.9492%
3	0x7791e137e62dcf5c408d003b9c9913c00e8f7e26	1,500,000,000	20.0000%
4	0xd9d1dbbe9530faaaa9e7d8fde0382eb00133696f	1,500,000,000	20.0000%
5	0x7d2d2bc5fb453673c3e31c6b002ef78613165cdc	209,949,557.02840506	2.7993%
6	0xd28526c1216f6954839f65adfeccb19bd86c403d	9,999,999	0.1333%
7	0xce55977e7b33e4e5534bd370ee31504fc7ac9adc	5,174,944.813335539345401989	0.0690%
8	0x93ab80c23be789f135c1bec19b5abf6f5a5446b9	600,000	0.0080%
9	0x03916d88c43de29efc535fa2bed631c0f16e0252	569,087.997039095175405941	0.0076%
10	0x4e368f4bca2960dc45f01867233fa67d0e9470d1	549,143.13312201	0.0073%

Contract functions details

+ [Int] IERC20
    -[Ext]totalSupply
    -[Ext]decimals
    -[Ext]symbol
    -[Ext]name
    -[Ext]getOwner
    -[Ext]balanceOf
    -[Ext]transfer#
    -[Ext]allowance
    -[Ext]approve#
    -[Ext]transferFrom#

+ Context
    -[int]<constructor >
    -[int]_msgsender
    -[int]_msgData

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

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

+ASYAGRO (Context, IERC20, Ownable)
    -[Pub]<Constructor>#
    -[Ext] getOwner
    -[Ext] decimals

Contract functions details

-[Ext] symbol
-[Ext] name
-[Ext] totalsupply
-[Pub] balanceOf
-[Ext] transfer#
-[Ext] allowance
-[Ext] approve#
-[Ext] transferFrom#
-[Pub] increaseAllowance #
-[Pub] decreaseAllowance #
-[Pub] burn #
    -Modifier: onlyOwner
-[Pub] mint #
    -Modifier: onlyOwner
-[Pub] freezeAccount #
    -Modifier: onlyOwner
-[Pub] lock #
    -Modifier: onlyOwner
-[Pub] lockDetail #
-[Ext] extendLockTime #
    -Modifier: onlyOwner
-[Ext] reduceLockTime #
    - Modifier: onlyOwner
-[Ext] unlockToken #
    - Modifier: onlyOwner
-[Ext] releaseLock #
    - Modifier: onlyOwner
-[Int] _transfer #
    - Modifier: onlyOwner
    -[Int] _burn #
    -[Int] _mint #
    -[Int] _approve #

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Passed
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.	Critical, High
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Medium issue
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

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

Four critical severity issue found.

1. Methods execution permissions.

Owners can mint tokens.

- **Description**

  According to the tokenomics maximum total supply is 7,500,000,000 ASY, but owners can mint more tokens using the mint function.

- **Location**

  Mint function

- **Recommendation**

  We advise to remove the ability to mint more than stated in tokenomics.

Owners can lock all tokens of any user anytime.

- **Description**

  Lock functionality should be limited by clear contract rules. Owners should not be able to block user tokens at their discretion.

- **Location**

  Lock function

- **Recommendation**

  We advise to change lock functionality.

Owners can change the lock time after the lock is created.

- **Description**

  The ability to change the lock time of an already created lock can lead to various manipulations.

- **Location**

  extendLockTime, reduceLockTime functions.

- **Recommendation**

  We advise to remove the ability to change the lock time after the lock is created.

Owners can unlock tokens anytime.

- **Description**

  he ability to unlock tokens for any account at any time can lead to various manipulations.

Security Issues

- **Location**

  unlockToken, releaseLock functions

- **Recommendation**

  We advise to remove the ability to unlock tokens before the end of the lock period.

High Severity Issues

One high severity issue found.

1. Methods execution permissions.

Highly permissive owner access

- **Description**

  Owners can add the user's address to the 'frozen' list. All ASY token transfers from such addresses will be reverted. This can lead to various manipulations and even loss of funds by users.

- **Location**

  freezeAccount function

- **Recommendation**

  We advise to remove the possibility to block the user’s funds.

Medium Severity Issues

One Medium severity issue found.

1. Scoping and Declarations.

Unused function.

- **Description**

  The freezeAccount function does nothing.

- **Location**

  freezeAccount function

- **Recommendation**

  We advise to remove unused code.

Low Severity Issues

One low severity issue found.

Owner Privileges

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

- ASYAGRO Contract:
    - Owner can renounce ownership.
    - Owner can transfer ownership.
    - Owner can burn tokens.
    - Owner can mint tokens.
    - Owner can freeze account.
    - Owner can lock tokens of address for given period.
    - Owner can extend lock time.
    - Owner can reduce lock time.
    - Owner can unlock tokens.
    - Owner can release lock.
    - Owner can transfer and lock tokens.

Conclusion

Smart contract contains low severity issues!

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.