HackSafe

Smart Contract Security Audit Report

Agrolot Token

January 2023

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
Agrolot Token

Deployer address
0xd54606bbf6ebb8c902bd97a2eef5d3702f1b699d

Client contacts
Agrolot Token

Blockchain
Ethereum

Website
Not provided

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 Agrolot Token to perform an audit of smart contracts:

- https://etherscan.io/token/0xfc05987bd2be489accf0f509e44b0145d68240f7#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 16.01.2023

Token Type	: DEFI
Contract name	: AgrolotToken
Contract address	: 0x72c9Fb7ED19D3ce51cea5C56B3e023cd918baaDf
Total supply	: 100,000,000
Token ticker	: AGLT
Decimals	: 18
Token Holders	: 82
Transactions count	: 868
Compiler version	: v0.4.24+commit.e67f0147
Contract deployer address	: 0xd54606bbf6ebb8c902bd97a2eef5d3702f1b699d
Owner address	: 0xd54606bbf6ebb8c902bd97a2eef5d3702f1b699d

Audit Summary

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

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 0 low.

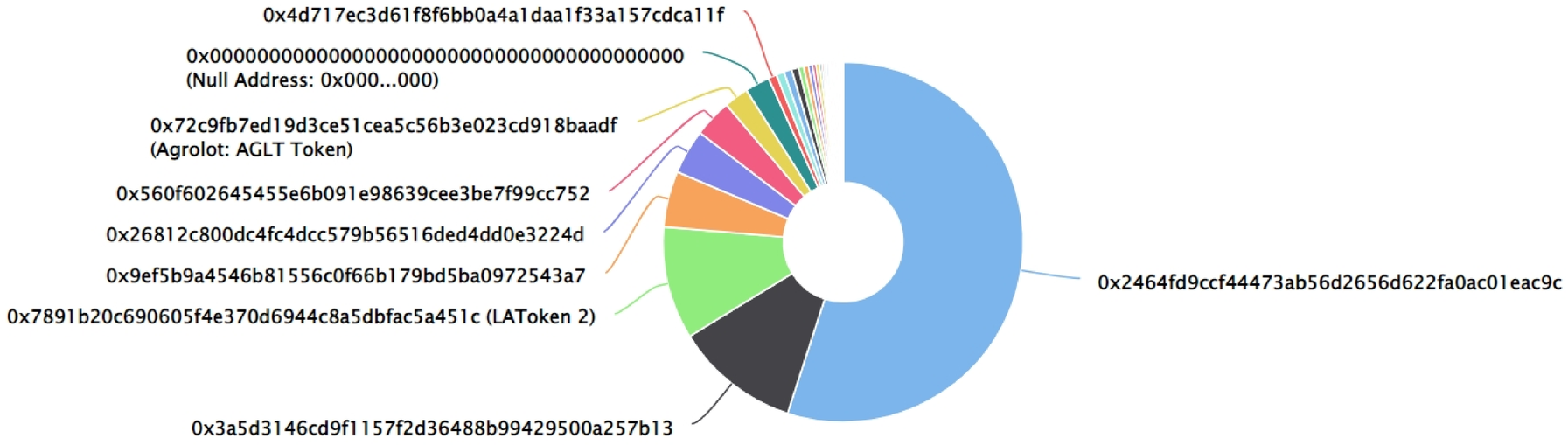
AgrolotToken Token Distribution

The top 100 holders collectively own 100.00% (100,000,000.00 Tokens) of Agrolot Token

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 82

Agrolot Token Top 100 Token Holders

Source: Etherscan.io



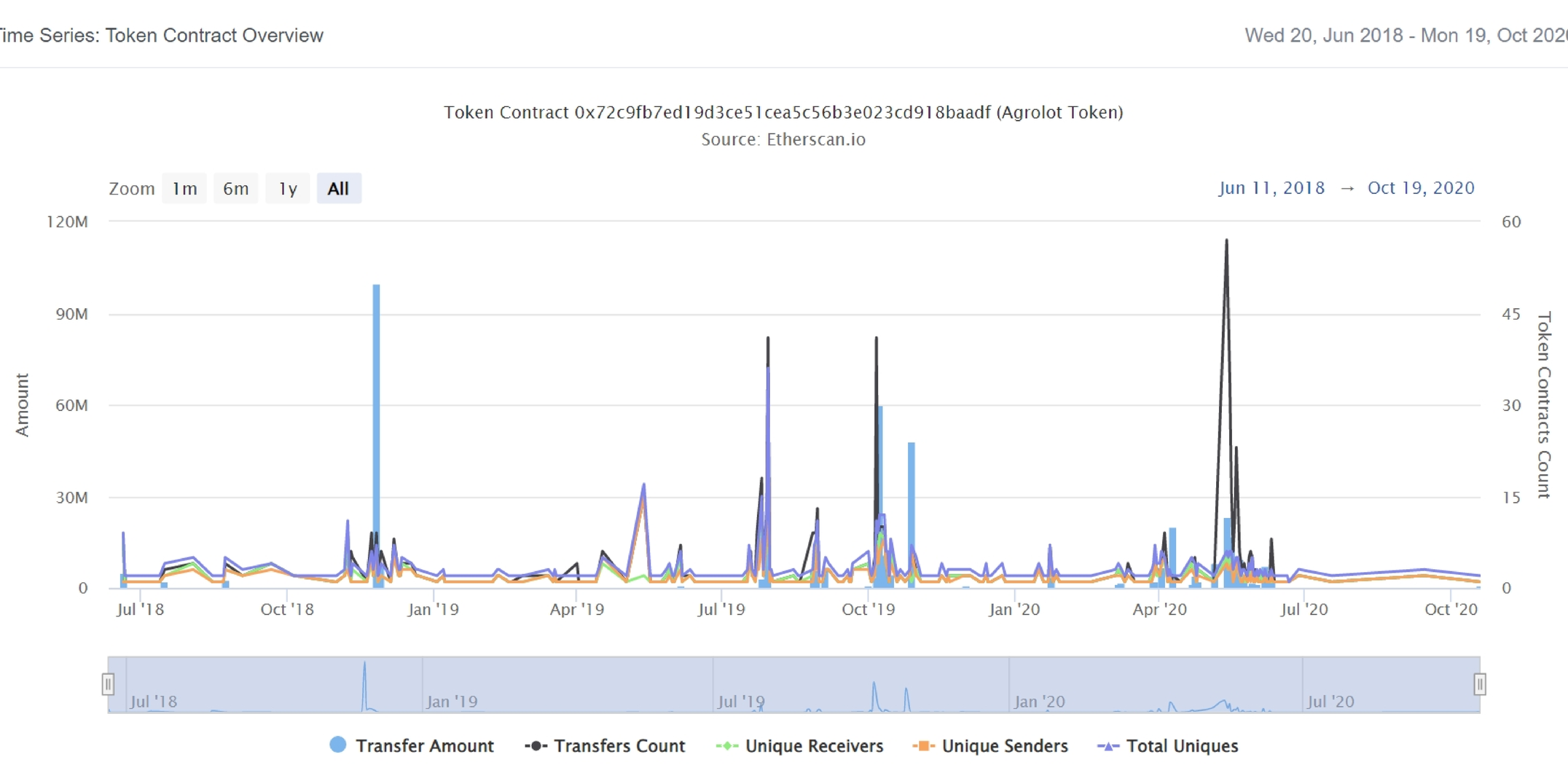
AgrolotToken Top 20Token Holders

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

Rank	Address	Quantity (Token)	Percentage
1	0x2464fd9ccf44473ab56d2656d622fa0ac01eac9c	54,993,510.02319171	54.9935%
2	0x3a5d3146cd9f1157f2d36488b99429500a257b13	11,248,461.075	11.2485%
3	LAToken 2	10,124,131.5457493399999996	10.1241%
4	0x9ef5b9a4546b81556c0f66b179bd5ba0972543a7	4,999,000	4.9990%
5	0x26812c800dc4fc4dcc579b56516ded4dd0e3224d	4,018,320.8715556	4.0183%
6	0x560f602645455e6b091e98639cee3be7f99cc752	3,399,990	3.4000%
7	Agrolot: AGLT Token	2,210,000	2.2100%
8	Null Address: 0x000...000	2,197,271	2.1973%
9	0x4d717ec3d61f8f6bb0a4a1daa1f33a157cdca11f	764,372.88582502	0.7644%
10	0x1d36905995376a6ccf9a90b9b33223128555bd43	722,772	0.7228%
11	0xee61f5fb0db81d3a09392375ee96f723c0620e07	694,878.3646992500000004	0.6949%
12	0xc9a06cb9750edb5f4b2a706895139f413d1a221d	634,728	0.6347%
13	0xf3f337eddfc68fa1a26d38f587478893277122b2	468,606.07432791	0.4686%
14	0xbc31ef24d2a4ee3e50700a68b248947b34515279	427,549	0.4275%
15	0xf31d363d6c891e3297384388b056b8cd6f83e068	376,023.74501169	0.3760%
16	0x5daa2aab0fda4fbd27f026410e92fcfc35047dd2	317,235	0.3172%
17	0x00343217b01188388c0e3242278231ace35e1b61	309,134.13328856	0.3091%
18	0x9152e4b206f5bbd581c85b780306b2efa86b8ed4	207,342.6	0.2073%
19	0x39d4e1789dd15c6f673eee11ea8db4ac122d66da	197,760	0.1978%
20	0x1718e503b10a538e7816c16a0093164246850438	191,480.5825	0.1915%

AgrolotToken Token Distribution

AgrolotToken Contract Overview



Contract functions details

+ERC20Basic
  -[Pub] balanceOf
  -[Pub] transfer

+ERC20 (ERC20Basic)
  -[Pub] allowance
  -[Pub] transferFrom
  -[Pub] approve

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

+BasicToken (ERC20Basic)
  -[Pub] transfer #
  -[Pub] balanceOf

+StandardToken (ERC20, BasicToken)
  -[Pub] transferFrom #
  -[Pub] approve #
  -[Pub] allowance

+Ownable
  -Ownable #
  -transferOwnership #
    -modifiers: onlyowner

+AgrolotToken (StandardToken)
  -AgrolotToken #

+Crowdsale (Ownable)
  -Crowdsale #
  -createTokens $
    -modifiers: saleison
  -[Ext] $
  -[Pub] getVIATokens #
  -[Pub] getTeamTokens #

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	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.	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**
  No low severity issue found.

Centralization

Owner Privileges :

- Agrolot Token Contract :
    - owner can transfer ownership

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 not create trouble as owner cannot modify any other functions of contract other than transferOwnership.

Conclusion

Smart contract contains no 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.