HackSafe

Smart Contract Security Audit Report

EROSCOIN

September 2022

Security Status

★ ★ ★ ★ ⯪

www.hacksafe.io

Audit Details

Audited project
EROSCOIN

Deployer address
0xC4faA76257F4310ec0125E3833eBc116afcE631a

Client contacts
EROSCOIN team

Blockchain
Ethereum

Website
https://eroscoin.org/

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 EROSCOIN to perform an audit of smart contracts:

- https://etherscan.io/token/0x74ceda77281b339142a36817fa5f9e29412bab85#code

The purpose of the audit was to achieve the following:

- Ensutre 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 27.09.2022

Token Type	: ERC20
Contract name	: EROSCOIN
Contract address	: 0x74CEDa77281b339142A36817Fa5F9E29412bAb85
Total supply	: 240,000,000
Token ticker	: ERO
Decimals	: 8
Token holders	: 1,737
Transactions count	: 7,372
Compiler version	: v0.4.16+commit.d7661dd9
Contract deployer address	: 0xC4faA76257F4310ec0125E3833eBc116afcE631a
Owner address	: 0xC4faA76257F4310ec0125E3833eBc116afcE631a

Social profiles

Twitter Profile	: https://twitter.com/eroscoinnews
Facebook profile	: https://www.facebook.com/eroscoin/
Github Profile	: https://github.com/eroscoin
Telegram Profile	: https://t.me/eroscoinplatform
Coinmarketcap profile	: https://coinmarketcap.com/currencies/eroscoin/

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “Secure”. This token contract does contain owner control, which do not make it fully decentralized as owner does 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, 0 medium and 2 low and some very low-level issues. These issues are not critical ones.

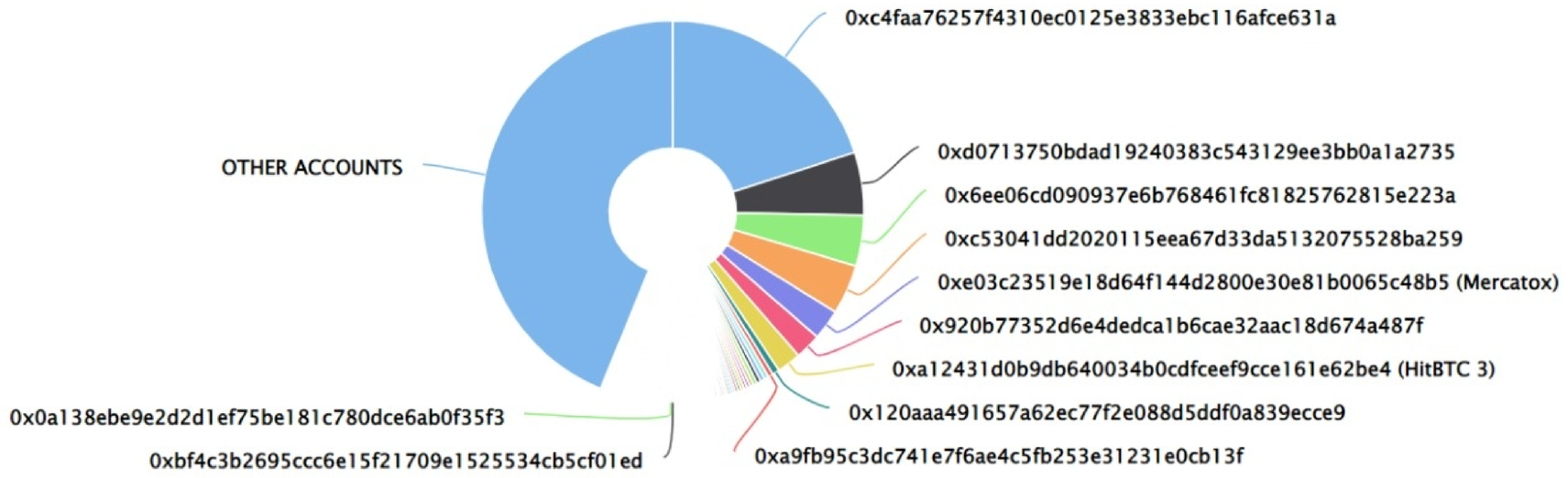
EROSCOIN Token Distribution

The top 100 holders collectively own 56.17% (134,803,820.74 Tokens) of EROSCOIN

Token Total Supply: 240,000,000.00 Token | Total Token Holders: 1,737

EROSCOIN Top 100 Token Holders

Source: Etherscan.io



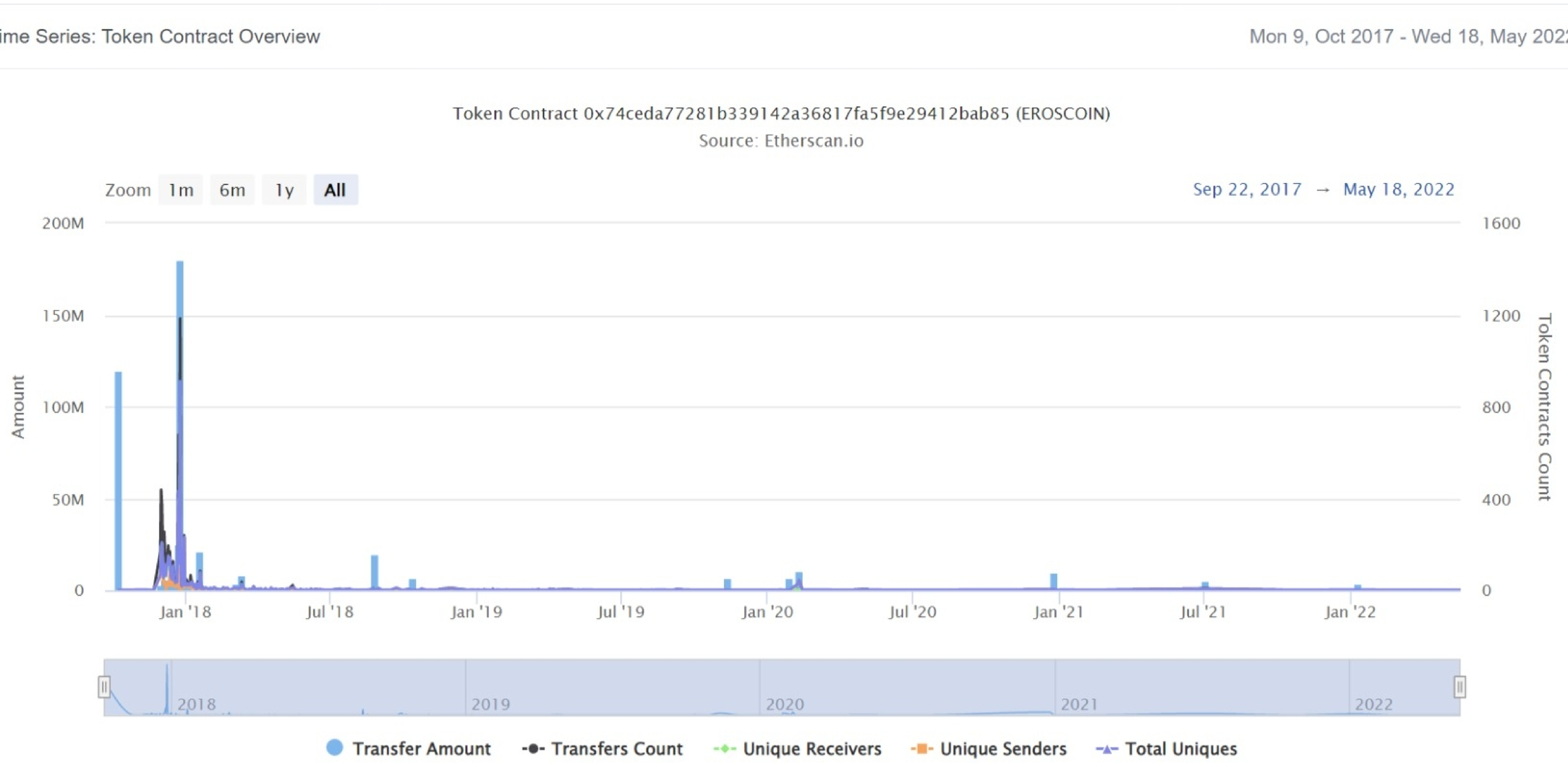
EROSCOIN Top 20 Token Holders

(A total of 134,803,820.74 tokens held by the top 100 accounts from the total supply of 240,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xc4faa76257f4310ec0125e3833ebc116afce631a	48,000,000	20.0000%
2	0xd0713750bdad19240383c543129ee3bb0a1a2735	12,771,800.53996596	5.3216%
3	0x6ee06cd090937e6b768461fc81825762815e223a	10,298,216.85966435	4.2909%
4	0xc53041dd2020115eea67d33da5132075528ba259	10,108,319.93871224	4.2118%
5	Mercatox	6,184,585.9488654	2.5769%
6	0x920b77352d6e4dedca1b6cae32aac18d674a487f	5,256,000	2.1900%
7	HitBTC 3	4,897,372.44077973	2.0406%
8	0x120aaa491657a62ec77f2e088d5ddf0a839ecce9	1,438,300	0.5993%
9	0xa9fb95c3dc741e7f6ae4c5fb253e31231e0cb13f	995,981	0.4150%
10	0x4f827d0776afb498bf8584ef8ff52f7a40c0c37f	945,690	0.3940%
11	0xf4d182afb69f20127c72abe265e436837474c8b7	899,480	0.3748%
12	0x2496b0cb8163a0ffe51727aa0264c5bccfbc7cc6	845,490.0169098	0.3523%
13	0x550c1498d61580e3b14bf97cc6d1da9eed5b3222	789,850	0.3291%
14	0x8622a6262f6497124259e7a5a4ebb760cbe79f92	676,904	0.2820%
15	0x1c2c6643cbae9a6f42fb83eba2c06c7cea28faed	655,701	0.2732%
16	0x6d56e2bbd347822a597c7807b7f36d58955d20f4	626,610	0.2611%
17	0xdaf10088f4c59e0cb25706350a8711f728fb8b27	625,395	0.2606%
18	0x8a1eaa75c237dc6dd173c48c9c4b6d02d55907c4	596,550	0.2486%
19	0x454dab0878932499a8af1fdfa1dafdfd38591a1f	591,520	0.2465%
20	0xe4a6084080e348f82360f0fbeb40e596390fb585	589,852	0.2458%

EROSCOIN Token Distribution

EROSCOIN Contract overview



Contract functions details

+ EROSCOINToken
    - balanceOf
    - transfer
    - transferFrom
    - approve
    - allowance

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

+ Ownable
    - Ownable
    - transferOwnership #
      -modifiers: onlyOwner
    - acceptOwnership #

+ EroStandardToken (EROSCOINToken, Ownable)
    - balanceOf
    - freezeAccount #
      -modifiers: onlyOwner
    - transfer #
    - transferFrom #
    - approve #
    - allowance

+ EROSCOIN (EroStandardToken)
    - EROSCOIN
    - approveAndCall

($) = 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.	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	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 issues found.

- **Medium Severity Issues**
  No medium severity issues found.

- **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 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 ^0.4.16 the contract should contain the following line:

  pragma solidity 0.4.16;

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.

Centralization

Owner Privileges :

- EROSCOIN ontract:
    - Owner can transfer ownership.
    - Owner can freeze account.

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 create trouble but smart contract ownership has been renounced. Following are Admin functions and burner functions:

- Transferownership
- Freezeaccount

Conclusion

Smart contract contains low 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.