HackSafe

Smart Contract Security Audit Report

Proton Token

February 2023

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
Proton Token

Deployer address
0x0170b8fd096d711f6f0cccddc5c25cb3eb550fa3

Client contacts
Proton Token Team

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 Proton Token to perform an audit of smart contracts:

- https://etherscan.io/token/0x4689a4e169eb39cc9078c0940e21ff1aa8a39b9c#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 08.02.2023

Token Type	: DEFI
Contract name	: MyToken
Contract address	: 0x4689a4e169eB39cC9078C0940e21ff1Aa8A39B9C
Total supply	: 10,000,000,000
Token ticker	: PTT
Decimals	: 18
Token Holders	: 80,850
Transactions count	: 191,674
Compiler version	: v0.4.18+commit.9cf6e910
Contract deployer address	: 0x0170b8fd096d711f6f0cccddc5c25cb3eb550fa3
Owner address	: 0xB2D52fE78541D8C926f80719c7D53B3eFdAFB7FD

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.

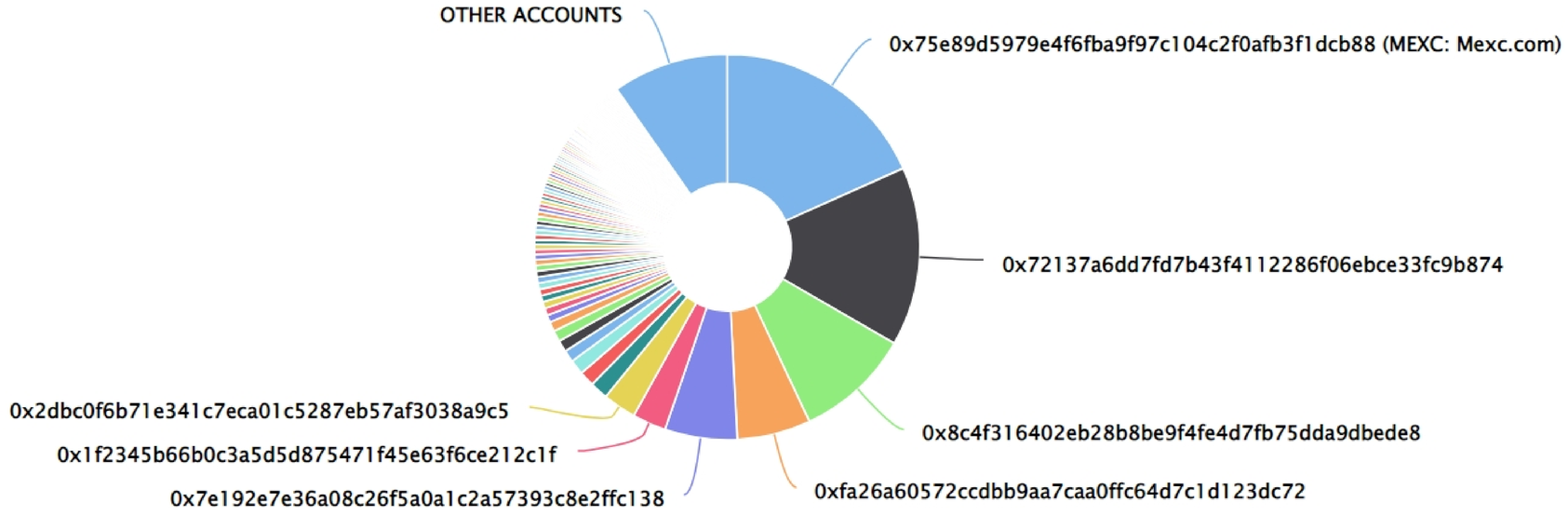
We found 0 critical, 0 high, 0 medium and 1 low.

PROTON TOKEN Token Distribution

The top 100 holders collectively own 90.27% (9,027,186,840.31 Tokens) of Proton Token | Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 80,850

Proton Token Top 100 Token Holders

Source: Etherscan.io



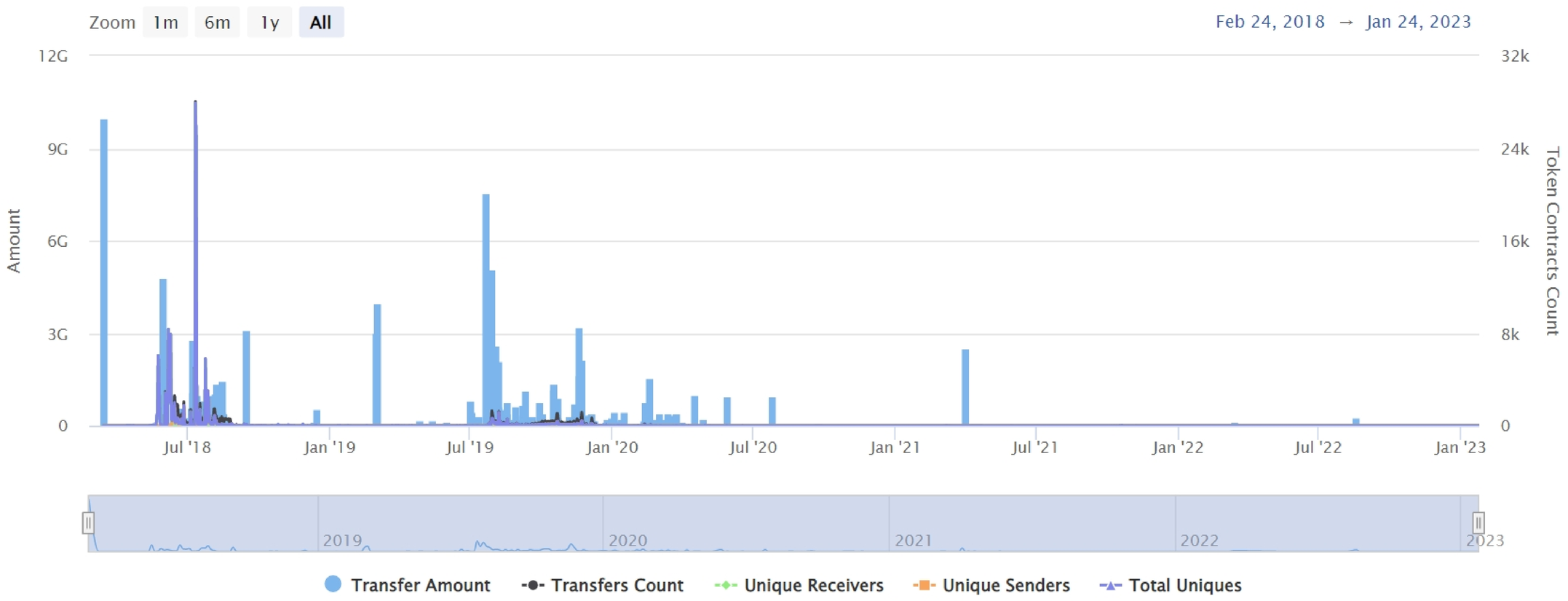
PROTON TOKEN Top 20 Token Holders

(A total of 9,027,186,840.31 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	MEXC: Mexc.com	1,832,298,743.013908882067589634	18.3230%
2	0x72137a6dd7fd7b43f4112286f06ebce33fc9b874	1,500,000,000	15.0000%
3	0x8c4f316402eb28b8be9f4fe4d7fb75dda9dbede8	968,145,700	9.6815%
4	0xfa26a60572ccdbb9aa7caa0ffc64d7c1d123dc72	617,595,247	6.1760%
5	0x7e192e7e36a08c26f5a0a1c2a57393c8e2ffc138	608,000,000	6.0800%
6	0x1f2345b66b0c3a5d5d875471f45e63f6ce212c1f	282,997,800	2.8300%
7	0x2dbc0f6b71e341c7eca01c5287eb57af3038a9c5	280,269,180.03	2.8027%
8	0xddb7db2f8db25501a23cd85a05541a5c0a523d15	150,461,750.52	1.5046%
9	0xcb5bc886a542cfc415a87498af62bc1bab1a6186	127,291,380.90653	1.2729%
10	0xa13fe037c3dc1bb137f456022ffb3596d2e812cc	125,968,354	1.2597%
11	0xe0befbbf63a53833bfc071d790bd85e36510a4bf	100,568,147	1.0057%
12	0xe179afcce34c2a67c3e2a9db00a4f28b3313e68d	97,526,819.69	0.9753%
13	0xe7ee7802b085f2ee42dbb84e222b494023822d63	92,134,459	0.9213%
14	0x2cc92e75f1980363c261ed3de0f616f8ed50ca71	81,047,303.6814	0.8105%
15	0x761e48fc976035d922a4004de485073f95f59b5f	60,581,396.23	0.6058%
16	0xc33a6fc58e92c552c4bc81dc42cb6c97ec7921f0	60,000,000	0.6000%
17	0x2543e9dd96091fb9f608d7471a4214569e17d8fb	56,267,135.82231629249087507	0.5627%
18	0xcb0952a458a1f6159e970565f7e6226dd4946404	53,682,368.26	0.5368%
19	0x92bf99f5b1d1c1c74a8393fc612081c52d85094f	52,991,104.64	0.5299%
20	0x8dfd918891ec63e8b11428ec80ff6ac014b8a3e4	52,695,658.4	0.5270%

PROTON TOKEN Token Distribution

PROTON TOKEN Contract Overview



Contract functions details

+SafeMath
  -[Int] safeMul
  -[Int] safeDiv
  -[Int] safesub
  -[Int] safeAdd

+owned
  -[Pub] owned
  -[Pub] transferOwnership #
    -modifier: onlyOwner

+[Int] tokenRecipient
  -[Ext] receiveApproval

+TokenERC20 (SafeMath)
  -[Pub] TokenERC20 #
  -[Int] _transfer #
  -[Pub] transfer #
  -[Pub] transferFrom #
  -[Pub] approve #
  -[Pub] approveAndCall #

+MyToken (owned, TokenERC20)
  -[Pub] MyToken #
  -[Pub] _transfer #
  -[Pub] burnFrom #
    -modifiers: onlyOwner
  -[Pub] burn #
    -modifiers: onlyOwner
  -[Pub] freezeAccount #
    -modifiers: onlyOwner
  -[Pub] $
  -[Pub] withdrawEther #
    -modifiers: onlyOwner
  -[Pub] withdrawMytoken #
    -modifiers: onlyOwner

($) = 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	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**
  NO medium severity issue found.
- **Low Severity Issues**
  One low severity issue found.

1. 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:

- Proton Token Contract:
    - Owner can transfer ownership.
    - Owner can burn tokens.
    - Owner can freeze Account.
    - Owner can withdraw Ether.
    - Owner can withdraw contract tokens.

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 as smart contract ownership has not been renounced. Following are Admin functions:

- transferOwnership
- withdrawMytoken
- withdrawEther
- freezeAccount
- burn
- burnFrom

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.