HackSafe

Smart Contract Security Audit Report

Torum

April **2022**

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
Torum

Deployer address
0xb8c02A851b095956aeC31C1C8D42268b3D3A30C6

Client contacts
Torum team

Blockchain
Binance Smart Chain

Website
https://www.torum.com/

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 Torum to perform an audit of smart contracts:

- https://bscscan.com/address/0xcd1faff6e578fa5cac469d2418c95671ba1a62fe#code

Contract Details

Token contract details for 19.04.2022

Contract name	: Torum
Contract address	: 0xCd1fAFf6e578Fa5cAC469d2418C95671bA1a62Fe
Total supply	: 800 million
Token Ticker	: XTM
Decimals	: 18
Token Holders	: 12,127
Transactions count	: 156, 715
Contract deployer address	: 0xb8c02A851b095956aeC31C1C8D42268b3D3A30C6
Owner address	: 0xb8c02A851b095956aeC31C1C8D42268b3D3A30C6

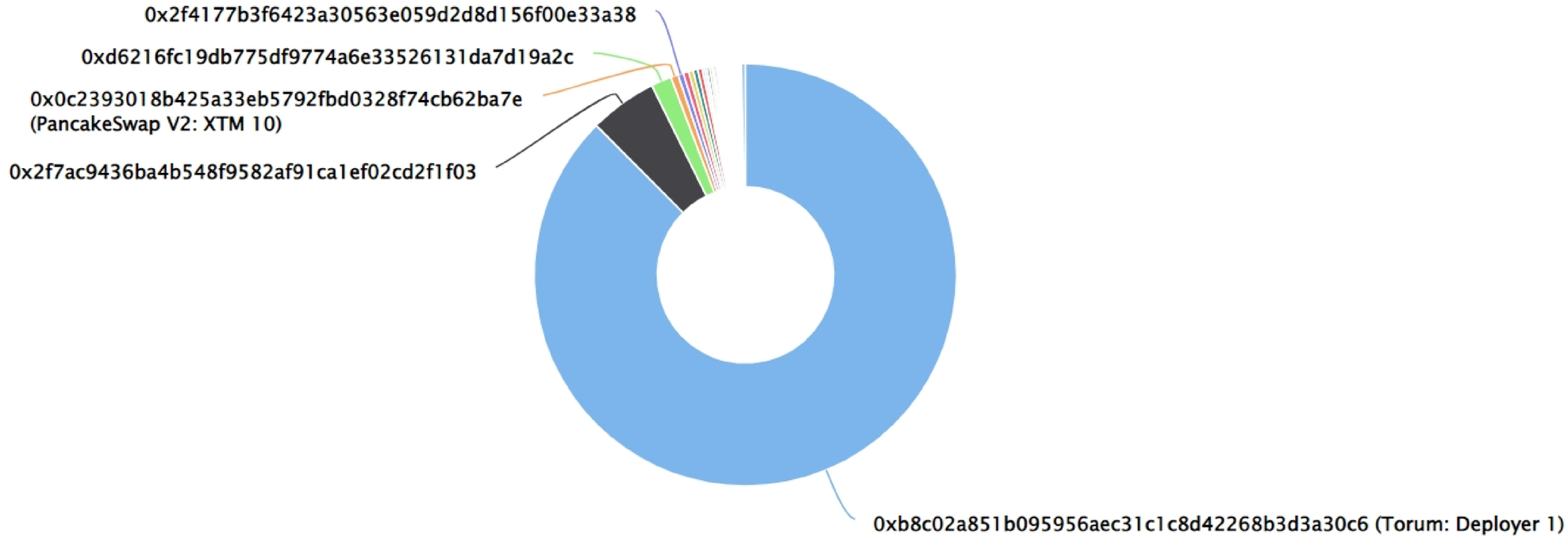
Torum Token Distribution

The top 500 holders collectively own 99.72% (797,771,731.50 Tokens) of Torum

Token Total Supply: 800,000,000.00 Token | Total Token Holders: 12,127

Torum Top 500 Token Holders

Source: BscScan.com



Torum Top 10 Token Holders

(A total of 775,203,852.12 tokens held by the top 10 accounts from the total supply of 800,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Torum: Deployer 1	700,099,974	87.5125%
2	0x2f7ac9436ba4b548f9582af91ca1ef02cd2f1f03	41,591,636.044831627179815911	5.1990%
3	0xd6216fc19db775df9774a6e33526131da7d19a2c	12,466,491	1.5583%
4	PancakeSwap V2: XTM 10	4,514,211.079844896670045678	0.5643%
5	0x2f4177b3f6423a30563e059d2d8d156f00e33a38	3,302,664	0.4128%
6	0x3bd629954cf029a07702359ee3298060d0362a75	3,284,334	0.4105%
7	0x300718a4af8f598077a212c8d9914c316ab0de68	2,916,664	0.3646%
8	0xd006534a5a6554154c7d27d14a2799ed43534899	2,781,214	0.3477%
9	0x71b38dc304b60276931360da59e3f9f4c82c0a60	2,746,664	0.3433%
10	0x06a586f0cc70e57bbcaeb1a2a0676f30f508500d	1,500,000	0.1875%

Contract functions details

Torum.sol
+ Torum (ERC20, Ownable)
    - <constructor> #

Ownable.sol
+ Ownable (Context)
    - <Constructor> #
    -[Pub] owner
    -[Pub] renounceOwnership #
      -modifiers: onlyOwner
    -[Pub] transferOwnership #
      -modifiers: onlyOwner
    -[Int] __setOwner #

ERC20.sol
+ ERC20 (Context, IERC20, IERC20Metadata)
    - <constructor> #
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer #
    -[Pub] allowance
    -[Pub] approve #
    -[Pub] transferFrom #
    -[Pub] increaseAllowance #
    -[Pub] decreaseAllowance #
    -[Int] _transfer #
    -[Int] _mint #
    -[Int] _burn #
    -[Int] _approve #
    -[Int] __beforeTokenTransfer
    -[Int] _afterTokenTransfer

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

Contract functions details

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

IERC20Metadata.sol
+ [Int] IERC20Metadata
    -[Ext] name
    -[Ext] symbol
    -[Ext] decimals

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.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Low 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

No critical severity issue found.

High Severity Issues

No high severity issue found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

One low severity issues found.

1. Scoping and Declarations.

Unused function.

- **Description**

  The _mint, _msgData functions do nothing.

- **Location**

  ERC20.sol -> _mint function
  Context.sol -> _msgData

- **Recommendation**

  We advise to remove unused code which can help you to develop clean coding style and save some computational gas too.

Owner Privileges

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

- Torum Contract:
    - Owner can transfer ownership.
    - Owner can renounce ownership.

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.