soken

SMART CONTRACT SECURITY AUDIT

BeforeCoinMarketCap

August, 2021

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws. We took into consideration smart contract based algorithms, as well. Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it. Before making any judgments, you have to conduct your own independent research. We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills). The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
- Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
- Hashes of all transaction will be recorded
- Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
- Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
- In this phase intended behaviour of smart contract is verified.
- In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
- Gas limits of functions will be verified in this stage.

4. Automated Testing:
- Mythril
- Oyente
- Manticore
- Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

- Low-severity issue — less important, must be analyzed
- Medium-severity issue — important, needs to be analyzed and fixed
- High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
- Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Token Contract Details for 18.08.2021

Contract Name: **BeforeCoinMarketCap**

Deployer address: **0xd5e2a54fef5f9e4a6b21ec646bbed7a160a00f18**

Total Supply: **8,553,027,612.5620464**

Token Tracker: **BCMC1**

Decimals: **18**

Token holders: **7,162**

Transactions count: **19,995**

Top 100 holders dominance: **99.86%**

Contract deployer address:
0xa3b43Ea19758bc79929dA12156866Ad26a5E136d

Audit Details

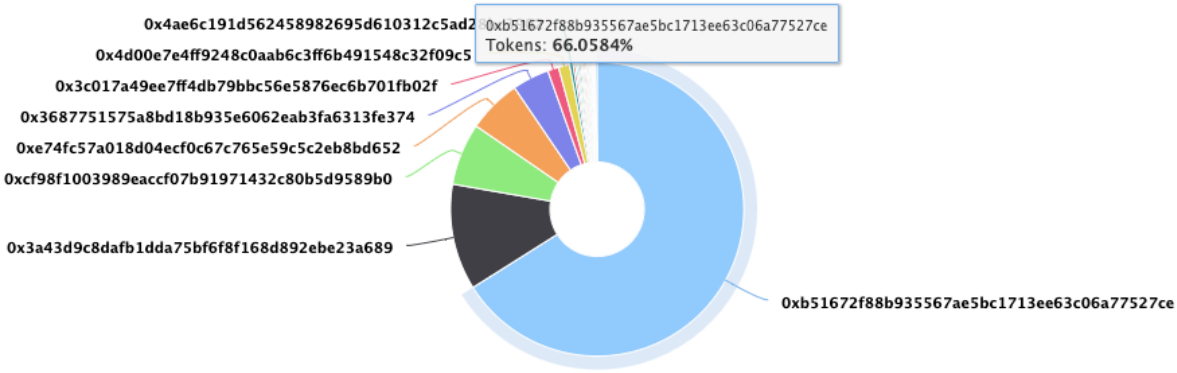
Project Name: **BeforeCoinMarketCap**

Language: **Solidity**

Blockchain: **Ethereum**

Project Website: **beta.beforecoinmarketcap.com**

BCMC1 Token Distribution



BCMC1 Top 10 Holders

Rank	Address	Quantity (Token)	Percentage
1	0xb51672f88b935567ae5bc1713ee63c06a77527ce	5,649,993,500	66.0584%
2	0x3a43d9c8dafb1dda75bf6f8f168d892ebe23a689	1,000,000,000	11.6918%
3	0xcf98f1003989eaccf07b91971432c80b5d9589b0	585,000,000	6.8397%
4	0xe74fc57a018d04ecf0c67c765e59c5c2eb8bd652	505,000,000	5.9043%
5	0x3687751575a8bd18b935e6062eab3fa6313fe374	346,347,434	4.0494%
6	0x3c017a49ee7ff4db79bbc56e5876ec6b701fb02f	105,000,000	1.2276%
7	0x4d00e7e4ff9248c0aab6c3ff6b491548c32f09c5	105,000,000	1.2276%
8	0x4ae6c191d562458982695d610312c5ad28bc3902	32,500,000	0.3800%
9	0x819cb5dddbb18f8c11c6baedacf0e0a9a6685632	21,275,393.67419	0.2487%
10	0xd051692701639366945fdab04e2ba47d7c2e0eb1	18,429,992	0.2155%

Contract Function Details

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

+ [Lib] Address.sol
- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Int] functionStaticCall #
- [Int] functionStaticCall #
- [Int] functionDelegateCall #
- [Int] functionDelegateCall #
- [Int] _verifyCallResult #

+ Ownable.sol (Context)
- [Pub] <Constructor> #
- [Pub] owner
- [Pub] onlyOwner
- [Pub] transferOwnership
- [Pub] _transferOwnership

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

- [Ext] decimals #
- [Ext] symbol
- [Ext] getOwner
- [Ext] balanceOf #

+ ERC20 is Context, IERC20
- [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] _setupDecimals
- [Int] _beforeTokenTransfer

+ [Lib] SafeERC20.sol
- [Int] safeTransfer
- [Int] safeTransferFrom
- [Int] safeApprove
- [Int] safeIncreaseAllowance
- [Int] safeDecreaseAllowance
- [Prv] _callOptionalReturn

+ IERC20Stake
- [Pub] _beforeTokenTransfer

+ IUsdMedianizer
- [Pub] read

+ BeforeCoinMarketCap is ERC20, Ownable
- [Ext] setStakeContract
- [Ext] BurnTokens
- [Int] _beforeTokenTransfer

($) = payable function
= non-constant function

Vulnerabilities checking Status

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Low-issues
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Security Issues

1) Outdated complier version issue:

The ABI specification uses pointers to data areas for everything that is dynamically-sized. Fixed in Solidity ^0.8.4.

2) Empty Byte Array Copy:

Copying an empty byte array (or string) from memory or calldata to storage can result in data corruption if the target array's length is increased subsequently without storing new data. Fixed in version > 0.7.4

3) Dynamic Array Cleanup issue:

When assigning a dynamically-sized array with types of size at most 16 bytes in storage causing the assigned array to shrink, some parts of deleted slots were not zeroed out. Fixed in version > 0.7.3.

Conclusion

Low-severity issues exist within smart contracts. Smart contracts are free from any critical or high-severity issues.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability.