soken

SMART CONTRACT SECURITY AUDIT

Manga Token

Scan and check this report was posted at Soken Github

April, 2022

Website: soken.io

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 12.04.2022

Contract Name: **MangaToken**

Deployed address: **0x8A88b501A68ceA5844B9d95F41892b05c4cd1d73**

Total Supply: **21,000,000**

Token Ticker: **MAN**

Decimals: **18**

Token holders: **22,921**

Transactions count: **94,227**

Top 100 holders dominance: **99.87%**

Audit Details

Project Name: **Manga Mon**

Language: **Solidity**

Compiler version: **v0.8.9**

Blockchain: **Fantom**

Social Profiles

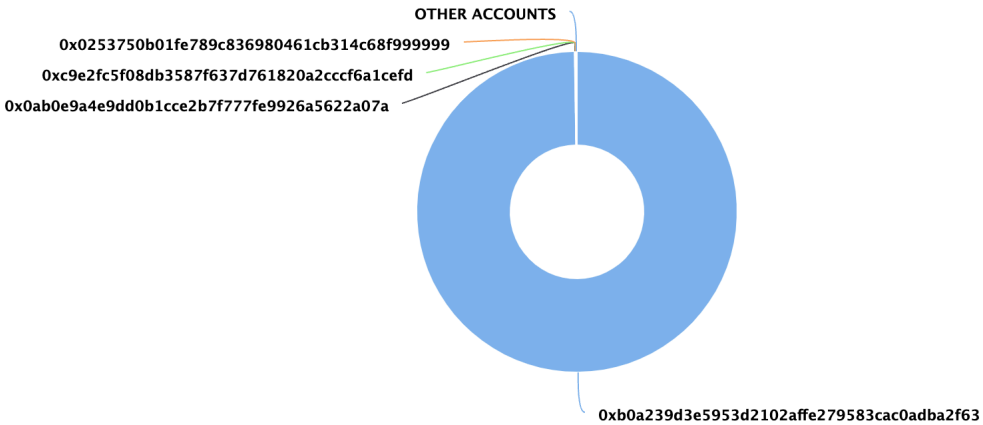
Project Website: **https://mangamon.io/**

Project Twitter: **https://twitter.com/mangamonjp**

Project Telegram Channel: **https://t.me/MangaMonOfficial**

Project Telegram Chat: **https://t.me/MangaMonchat**

MAN Token Distribution



MAN Top 10 Holders

Rank	Address	Quantity (Token)	Percentage
1	0xb0a239d3e5953d2102affe279583cac0adba2f63	20,953,000.000001001	99.7762%
2	0x0ab0e9a4e9dd0b1cce2b7f777fe9926a5622a07a	14,239	0.0678%
3	0xc9e2fc5f08db3587f637d761820a2cccf6a1cefd	1,689.050000301	0.0080%
4	0x0253750b01fe789c836980461cb314c68f999999	400.850000001	0.0019%
5	0xe6df221ac1a3e87a3a085a0395d73f7db41a375d	289.150000001	0.0014%
6	0x858df5108f14df54c163ac82bc3d5916e2666666	237.450000001	0.0011%
7	0x886244f12654d4b5850bde83e76fe5b94b054169	212.900000001	0.0010%
8	0xa4ad3d70d77b526abff61cbabbbc65fb202bcb2d	142.150000001	0.0007%
9	0x0652a26235b058ae22ba976bfe367a248e841f1f	93.700000001	0.0004%
10	0x3feb4a32ea00221e190463d041e0fecf594bb5c8	81.600000001	0.0004%

Vulnerabilities checking

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	Completed
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) PRESENCE OF OVERPOWERED ROLE : MangaToken.sol L322 - 329;

The overpowered owner (i.e., the person who has too much power) is a project design where the contract is tightly coupled to their owner (or owners); only they can manually invoke critical functions.

2) LOOP CONSUMING EXCESSIVE GAS : MangaToken.sol L169 - 177 && L243 - 247 && L327 - 328;

Ethereum is a very resource-constrained environment. Prices per computational step are orders of magnitude higher than with centralized providers. Moreover, Ethereum miners impose a limit on the total number of Gas consumed in a block. If ***array.length*** is large enough, the function exceeds the block gas limit, and transactions calling it will never be confirmed.

for (uint256 i = 0; i < array.length ; i++) {costlyFunc();}

This becomes a security issue, if an external actor influences ***array.length***.

E.g., if an array enumerates all registered addresses, an adversary can register many addresses, causing the problem described above.

Conclusion

Medium and low-severity issues have been found within the contract, contract is free from high-severity or critical issues.

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

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team