SECURICHAIN

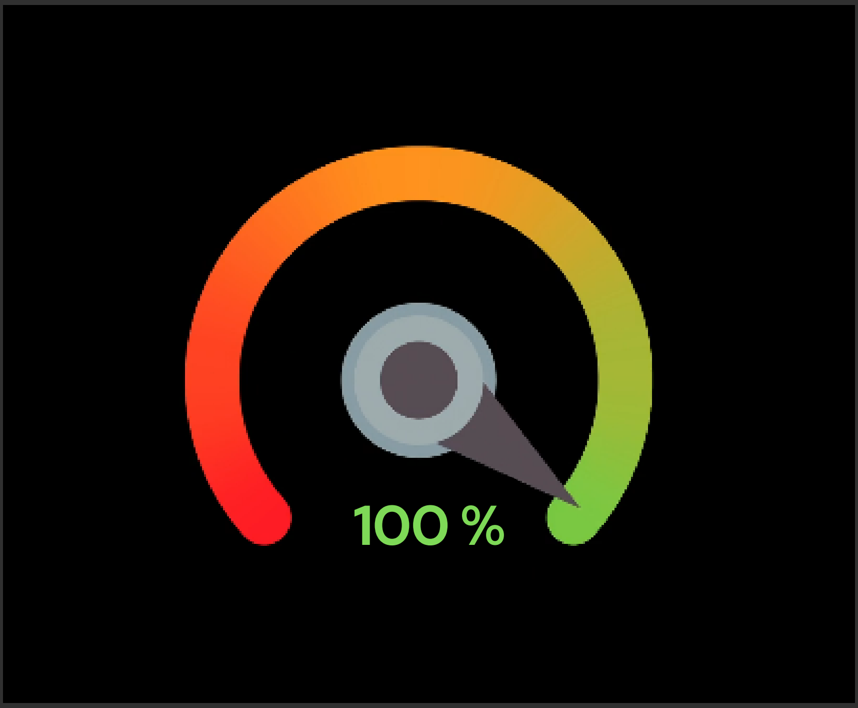
SMART CONTRACT AUDIT

SECURITY ANALYSIS REPORT
FOR

MYSTIC TREASURE CONTRACT

APRIL 07th , 2023

Security Rating



The rating is based on the number, severity and latest status of detected issues

DISCLAIMER

This report contains confidential information which can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed – upon a decision of the Customer.

SecuriChain does not provide any warranty or guarantee regarding the absolutely bug-free nature of the technology analyzed.

The report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

SECURICHAIN

TABLE OF CONTENTS

VULNERABILITY ASSESSMENT OVERVIEW

1.1. ASSIGNING RISK LEVELS

The Auditor categorizes each of the detected vulnerabilities into 4 levels (High, Medium, Low, and Info) according to the degree of the risks it may cause in the Customer's operations. For details of the rating standards, please refer to "Appendix 2 Risk Rating." Please also note that the assessment of the findings is based on Auditor's own perspective and may contain speculations in some cases.

1.2. SCOPE OF WORK

Project Name	MYSTIC TREASURE CONTRACT
Platform	Ethereum
Languages	Solidity
Methods	Automation scan, architecture review, functional testing, manual code review
Repository	https://bitbucket.org/Cu8/mystic-treasure-smart-contract/src/master/
Documents	
Timelines	April 03rd 2023 – April 07th 2023

1.3. CHECKSUM FILE

MYSTIC-TREASURE-CONTRACTS

No.	Hash (MD5)	Name
1	cd2dd043d321c41ad7245dd02c7407525afc1483c3d12ceb49959b01364f3e2a	contracts/daily-checkin/external/DateTime.sol
2	a74e79df80ccdd68f95657f2337a4af82581ac8125f17de2ab96d6b865b02639	contracts/daily-checkin/interfaces/IDateTime.sol
3	fd989a355f974e2127e2ef967e34a3dfa50f3ed68a55a6d6d6e9aa1865553c16	contracts/daily-checkin/interfaces/IDateTimeUtils.sol
4	cd2dd043d321c41ad7245dd02c7407525afc1483c3d12ceb49959b01364f3e2a	contracts/daily-checkin/DailyCheckIn.sol
5	6cd589e02a8401781e210cbf0f3288829917526fd5fdad337bd5fefba4136983	contracts/daily-checkin/DateTimeUtils.sol
6	358e22279e2deb3d5142a5dc710db8047ebc0494bb0a5ac403ecc523fbd43ff6	contracts/nft/Item.sol

1.3. CHECKSUM FILE

MYSTIC-TREASURE-CONTRACTS

No.	Hash (MD5)	Name
7	af9c659c3baec272f093738a413a6a2c3a7a3034462e69b0d98e00f06d226930	contracts/nft-marketplace/Marketplace.sol
8	ebd599b8f9390a93e293896c8a6ff697f927b5c3dd6d6f38ec60efe5363f163e	contracts/nft-marketplace/MarketplaceStorage.sol
9	f9dfda879c27c92bed40b4c624e17d566879bf8efde1a9a3019550f1f97a2ec1	contracts/payment/Payment.sol
10	a31ad9887840d87093569c019566b63a0e2ad47c496cace9f9f39a62f8534363	contracts/utils/VerifySign.sol
11	4fd6092bdfa8b42f19d535c5ac69c4323b0b894717c699e58d5552eeabd04cd4	contracts/Migrations.sol
12	b977d58ebd0a8252914c95068dd49f8e04aea9f978685fdb3e562881f3e8b7e7	contracts/MYTToken.sol

1.4. ASSESSMENT RESULTS

According to the assessment, the Customer's smart contracts have a security rating of 100/100

RATE	DESCRIPTION
96-100	**No vulnerabilities** were found or all detected ones have been resolved
70-95	Unresolved **Low-level** vulnerabilities exist
40-69	Unresolved **Medium-level** vulnerabilities exist
0-39	Unresolved **High-level** vulnerabilities exist

For more information on criteria for risk rating, refer to Appendix.2

FINDINGS

2.1 List of Vulnerabilities

The detected vulnerabilities are listed below. Please refer to "Appendix.2 Risk Rating" for the risk assessment method.

Vulnerabilities distributed in the smart contract

ID	Risk Level	Name	Amount	Status
SC1	Infomation	Unlocked Pragma	1	Resolved

For rating each vulnerability, refer to Appendix 2.

2.2 Details of the audit process

Automation scan

During the scanning process, we used automated tools that utilize 85 detectors of info-to-high level error detection, the following results were obtained:

Migrations.sol analyzed (1 contracts with 85 detectors), 4 result(s) found
MYTToken.sol analyzed (7 contracts with 85 detectors), 11 result(s) found
daily-checkin/ analyzed (28 contracts with 85 detectors), 149 result(s) found
nft/ analyzed (17 contracts with 85 detectors), 83 result(s) found
nft-marketplace/ analyzed (15 contracts with 85 detectors), 60 result(s) found
payment/ analyzed (16 contracts with 85 detectors), 79 result(s) found
utils/ analyzed (1 contracts with 85 detectors), 3 result(s) found

After verification, we identified the Unlocked Pragma as considerable while other vulnerabilities are false positives and could not be exploited (including vulnerabilities protected by libraries in @openzeppelin).

Manual code review

During the manual code review, no serious security issues were found in the following components:

Daily check-in: No security issues were detected. The date processing logic is sound. The check-in logic is reasonable and ensures that each player can only check in once per day.

NFT: No serious security issues were found. Functions such as deposit, withdraw, etc., lack a check to verify whether the tokenId already exists before creating or transacting. However, these have been checked by ERC721Upgradeable, making the transactions safe.

NFT-Marketplace: No serious security issues were found. The create/update/cancel/execute functions are handled and ownership is fully checked.

Payment: No serious security issues were found. The authentication of signers and execution of transactions are unlikely to create security issues.

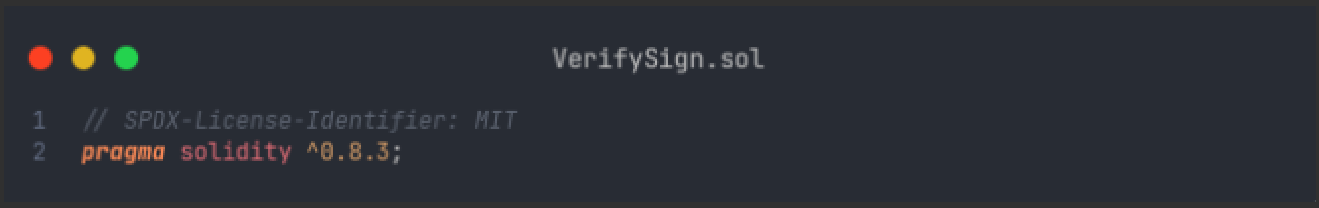
Migrations/MYToken: No serious security issues were found. The tokens are safely created based on the proposed template

2.2 Details of the audit results

Unlocked Pragma

Overview

Contracts should be deployed with the same compiler version and flags that they have been thoroughly tested. Locking the pragma helps to ensure that contracts do not accidentally get deployed using.



VerifySign.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.3;
```

An outdated compiler version that might introduce bugs that affect the contract system negatively.

Recommendation

Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the chosen compiler version.
Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

Location

Mystic: All Contract

CONCLUSION

This document, and its appendices, represent the results of several days of our intensive work.

Smart contracts within the scope were analyzed with static analysis tools and manually reviewed.

Please feel free to direct any questions on this assessment to: audit@securichain.io.

SECURICHAIN

APPENDIX 1: ASSESSMENT LIST

	CHECKLIST	
Arithmetic operations	Integer Overflow/Underflow	Integer Division
	Integer Truncation	Integer Sign
	Wrong Operator	
Re-entrancy		
Bad Randomness	Timestamp Dependence	Blockhash
Front running		
DDos	DOS By Complex Fallback Function	DOS By Gaslimit
	DOS By Non-existent Address Or Malicious Contract	
Unsafe external calls		
Gas usage	Invariants in Loop	Invariants State Variables Are Not Declared Constant
Business Logics Review		
Access Control & Authorization	Replay Attack	Use tx.origin For Authentication
Logic Vulnerability		

APPENDIX 2: LIST RATING

Risk Level	Explain	Example Types
High	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.	Re-entrancy Front running DDos Bad Randomness Logic Vulnerability Arithmetic operations
Medium	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.	Access Control Unsafe external calls Business Logics Review Logic Vulnerability
Low	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.	Gas Usage
Info	The issue does not pose an immediate risk, but is relevant to security best practices or Defense in Depth.	Do not specify a specific version of Solidity