Competitive Security Assessment

ModeMaxIO

Jun 24th, 2024

Secure3

secure3.io

Summary

This report is prepared for the project to identify vulnerabilities and issues in the smart contract source code. A group of NDA covered experienced security experts have participated in the Secure3′s Audit Contest to find vulnerabilities and optimizations. Secure3 team has participated in the contest process as well to provide extra auditing coverage and scrutiny of the finding submissions.
The comprehensive examination and auditing scope includes:
• Cross checking contract implementation against functionalities described in the documents and white paper disclosed by the project owner.
• Contract Privilege Role Review to provide more clarity on smart contract roles and privilege.
• Using static analysis tools to analyze smart contracts against common known vulnerabilities patterns.
• Verify the code base is compliant with the most up-to-date industry standards and security best practices.
• Comprehensive line-by-line manual code review of the entire codebase by industry experts.
The security assessment resulted in findings that are categorized in four severity levels: Critical, Medium, Low, Informational. For each of the findings, the report has included recommendations of fix or mitigation for security and best practices.

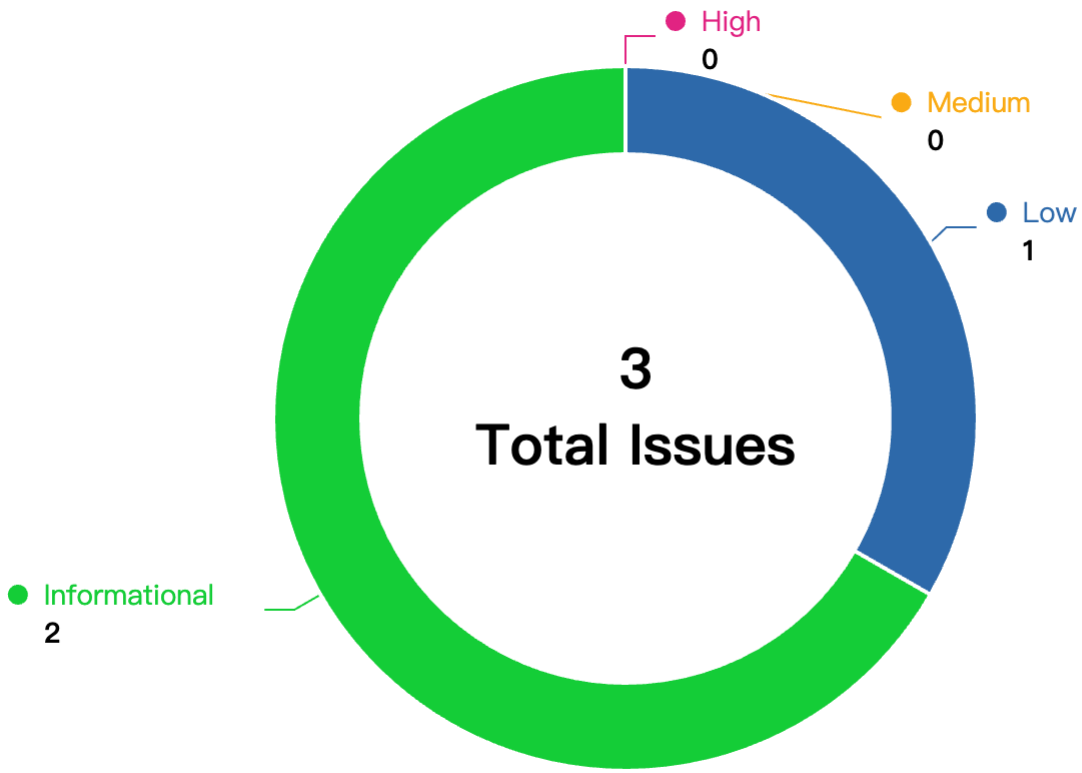
Overview

Project Name	ModeMaxIO
Language	solidity
Codebase	• https://github.com/ModeMaxIO/modemax-contracts.git • audit version - 2780d41a97a669df0d8af78a99a96db4dd67e78f • final version - 3185c57a51d453a818b999414e21c903611f0d37
Audit Methodology	• Audit Contest • Business Logic and Code Review • Privileged Roles Review • Static Analysis

Audit Scope

File	SHA256 Hash
contracts/oracle/ChainlinkAggregator4Pyth.sol	40e503cf2da692f38967a9f6b63435d2bbcb4880b9ef4b4007a9ae25dd6db00c
contracts/oracle/AdapterPyth.sol	18236161a59db3be5a2527d44894c8dc37bcf84668f6bebe224c2aba7c64ad92

Code Assessment Findings



ID	Name	Category	Severity	Client Response	Contributor
MMI-1	Lack of Zero Address Validation	Logical	Low	Fixed	0xCO2
MMI-2	`setKeeper` function should emit event	Logical	Informational	Fixed	toffee
MMI-3	State variables that could be declared immutable	Gas Optimization	Informational	Fixed	jiayeqian

MMI-1:Lack of Zero Address Validation

Category	Severity	Client Response	Contributor
Logical	Low	Fixed	0xCO2

Code Reference

- code/contracts/oracle/AdapterPyth.sol#L11-L13

```
11: constructor(address contractAddress) {
12:         pythContract = contractAddress;
13:     }
```

Description

0xCO2: Constructor of `AdapterPyth.sol` lacks zero address validation, since parameter of constructor are used to initialize state variable which are used in other function of the contract, error in these state variable can lead to redeployment of contract.

Recommendation

0xCO2: Add require condition to check for zero address.

Client Response

client response for 0xCO2: Fixed. We accept the recommendation. commit-3185c57a51d453a818b999414e21c903611f0d37.

MMI-2: `setKeeper` function should emit event

Category	Severity	Client Response	Contributor
Logical	Informational	Fixed	toffee

Code Reference

- code/contracts/oracle/ChainlinkAggregator4Pyth.sol#L34

```
34: function setKeeper(address _keeper, bool _isKeeper) external onlyOwner {
```

Description

toffee: `setKeeper` function is setting a critical state map but lacking event emission

Recommendation

toffee: emit an event when the map updated

Client Response

client response for toffee: Fixed. We accept the recommendation. commit-3185c57a51d453a818b999414e21c903611f0d37

MMI-3:State variables that could be declared immutable

Category	Severity	Client Response	Contributor
Gas Optimization	Informational	Fixed	jiayeqian

Code Reference

- code/contracts/oracle/AdapterPyth.sol#L9

```
9: address public pythContract;
```

Description

jiayeqian: State variables `pythContract` that are not updated following deployment should be declared immutable to save gas.

Recommendation

jiayeqian: Add the immutable attribute to state variables that never change or are set only in the constructor.

```
    address public immutable pythContract;
```

Client Response

client response for jiayeqian: Fixed. commit-3185c57a51d453a818b999414e21c903611f0d37

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Invoices, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Invoice. This report provided in connection with the services set forth in the Invoices shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Invoice. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without Secure3's prior written consent in each instance.

This report is not an "endorsement" or "disapproval" of any particular project or team. This report is not an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Secure3 to perform a security assessment. This report does not provide any warranty or guarantee of free of bug of codes analyzed, nor do they provide any indication of the technologies, business model or legal compliancy.

This report should not be used in any way to make decisions around investment or involvement with any particular project. Instead, it represents an extensive assessing process intending to help our customers increase the quality of their code and high-level consistency of implementation and business model, while reducing the risk presented by cryptographic tokens and blockchain technology.

Secure3's position on the final decisions over blockchain technologies and corresponding associated transactions is that each company and individual are responsible for their own due diligence and continuous security.

The assessment services provided by Secure3 is subject to dependencies and under continuing development. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.