FYEO

Security Assessment of the Abacus Monorepo Solidity Contracts

Abacus Works, Inc.

September 2022
Version 1.1

Presented by:
FYEO Inc.
PO Box 147044
Lakewood CO 80214
United States

Security Level
Strictly Confidential

Table of Contents

List of Figures

List of Tables

Executive Summary

Overview

Abacus Works, Inc. engaged FYEO Inc. to perform a Security Assessment of the Abacus Monorepo Solidity Contracts.

The assessment was conducted remotely by the FYEO Security Team. Testing took place on July 25 - August 05, 2022, and focused on the following objectives:

- To provide the customer with an assessment of their overall security posture and any risks that were discovered within the environment during the engagement.
- To provide a professional opinion on the maturity, adequacy, and efficiency of the security measures that are in place.
- To identify potential issues and include improvement recommendations based on the results of our tests.

This report summarizes the engagement, tests performed, and findings. It also contains detailed descriptions of the discovered vulnerabilities, steps the FYEO Security Team took to identify and validate each issue, as well as any applicable recommendations for remediation.

Key Findings

The following issues have been identified during the testing period. These should be prioritized for remediation to reduce to the risk they pose:

- FYEO-AB-01 – Known issues in compiler
- FYEO-AB-02 – Incomplete build instructions
- FYEO-AB-03 – Public visibility is set for functions that are not called internally

Based on our review process, we conclude that the reviewed code implements the documented functionality.

Scope and Rules of Engagement

The FYEO Review Team performed a Security Assessment of the Abacus Monorepo Solidity Contracts. The following table documents the targets in scope for the engagement. No additional systems or resources were in scope for this assessment.

The source code was supplied through a public repository at https://github.com/abacus-network/abacus-monorepo/tree/audit-scope-0/solidity/core/contracts with the commit hash 24dc33c976cc51364abc5f5a63cf5ce46b84bbf1.

A re-review was performed on August 22, 2022, with the commit hash 6196714ee488d3f7feab965126409f4b4660c8de.

Files included in the code review

```
abacus-monorepo/
└── solidity/
    └── core/
        └── contracts/
            ├── libs/
            │   ├── Merkle.sol
            │   ├── Message.sol
            │   └── TypeCasts.sol
            ├── test/
            │   ├── bad-recipient/
            │   │   ├── BadRecipient1.sol
            │   │   ├── BadRecipient2.sol
            │   │   ├── BadRecipient3.sol
            │   │   ├── BadRecipient5.sol
            │   │   └── BadRecipient6.sol
            │   ├── MysteryMath.sol
            │   ├── MysteryMathV1.sol
            │   ├── MysteryMathV2.sol
            │   ├── TestInbox.sol
            │   ├── TestMailbox.sol
            │   ├── TestMerkle.sol
            │   ├── TestMessage.sol
            │   ├── TestMultisigValidatorManager.sol
            │   ├── TestOutbox.sol
            │   ├── TestRecipient.sol
            │   ├── TestSendReceiver.sol
            │   └── TestValidatorManager.sol
            ├── upgrade/
            │   ├── UpgradeBeacon.sol
```

Files included in the code review
│ ├── UpgradeBeaconController.sol │ └── UpgradeBeaconProxy.sol ├── validator-manager/ │ ├── InboxValidatorManager.sol │ ├── MultisigValidatorManager.sol │ └── OutboxValidatorManager.sol ├── AbacusConnectionManager.sol ├── Inbox.sol ├── InterchainGasPaymaster.sol ├── Mailbox.sol ├── MerkleTreeManager.sol ├── Outbox.sol └── Version0.sol

Table 1: Scope

Technical Analyses and Findings

During the Security Assessment of the Abacus Monorepo, we discovered:

- 1 finding with LOW severity rating.
- 2 findings with INFORMATIONAL severity rating.

The following chart displays the findings by severity.

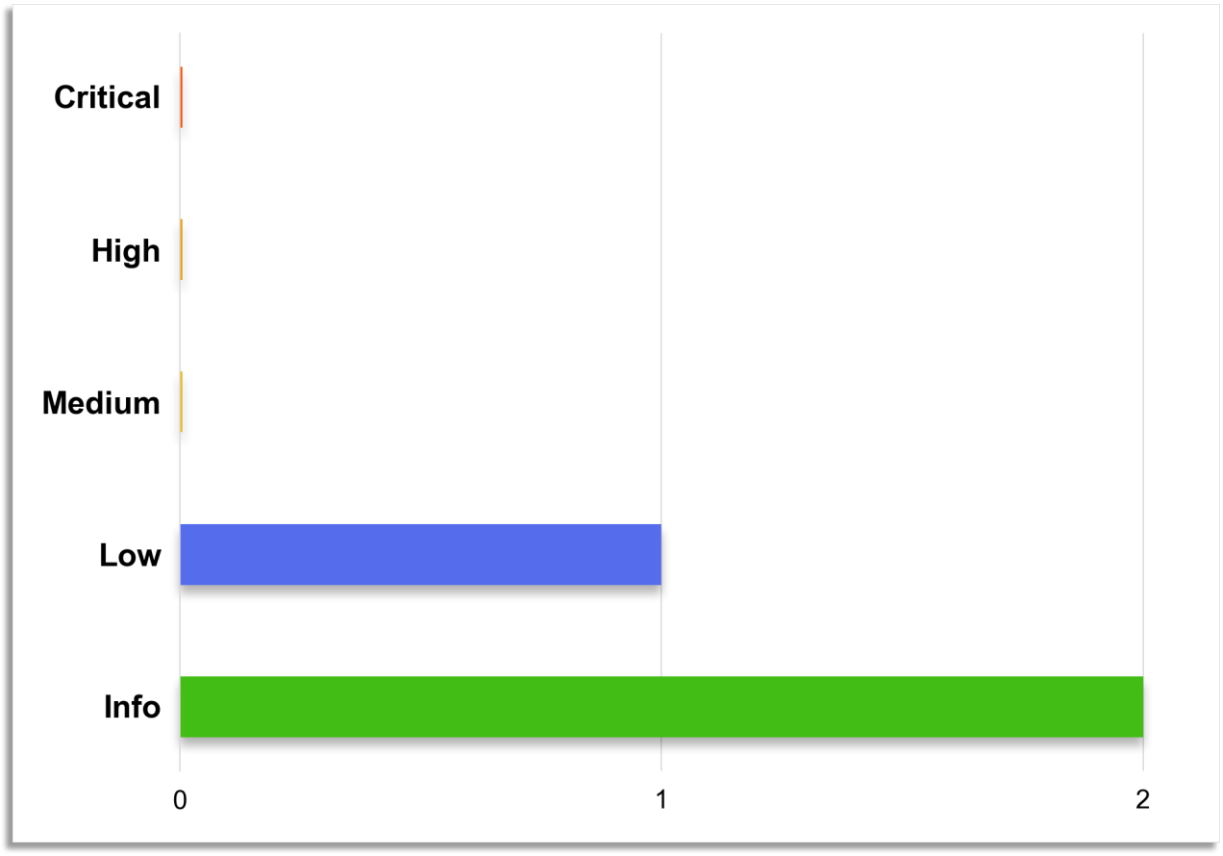

Figure 1: Findings by Severity

Findings

The *Findings* section provides detailed information on each of the findings, including methods of discovery, explanation of severity determination, recommendations, and applicable references.

The following table provides an overview of the findings.

Finding #	Severity	Description
FYEO-AB-01	Low	Known issues in compiler
FYEO-AB-02	Informational	Incomplete build instructions
FYEO-AB-03	Informational	Public visibility is set for functions that are not called internally

Table 2: Findings Overview

Technical Analysis

The source code has been manually validated to the extent that the state of the repository allowed. The validation includes confirming that the code correctly implements the intended functionality.

Based on our review process, we conclude that the code implements the documented functionality to the extent of the reviewed code.

Technical Findings

General Observations

Abacus is a platform that is built to allow interchain communication. The scope of the current review is the smart contract implementation written in Solidity.

The main entities in the platform are:

- **Message** - is a pack of data that has information about the origin, destination, sender, receiver, and the message data itself.
- **Incremental Merkle tree** - a GAS-efficient structure to keep existence proofs of all messages sent through the contract.
- **Outbox** - the mailbox to send messages from the current network to another.
- **Inbox** - the mailbox that receives and propagates incoming messages. Each supported chain has its own Inbox.
- **Validators** - the set of accounts that are responsible for the validation and signing of messages that will be transferred to another chain.
- **Interchain Gas Paymaster** - manages payments on a source chain to cover gas costs of relaying messages to destination chains

The current implementation has only one set of validators which makes it prone to fraud signers, however, it is stated that this would be improved in a future version with sovereign consensus - https://docs.useabacus.network/abacus-docs/protocol/security/sovereign-consensus. It is recommended to have another round of audits after this functionality is implemented.

The overall quality of the code is good. During the review, only some low and informational issues were found without a real threat to the platform functionality. The code is well structured and documented. Optimized algorithms are used, making the logic GAS efficient.

All the important scenarios and almost all lines of the code are covered with unit tests. The uncovered functions are `latestCachedCheckpoint` in `Outbox` and `_initialize` in `UpgradeBeaconProxy`.

KNOWN ISSUES IN COMPILER

Finding ID: FYEO-AB-01
Severity: Low
Status: Remediated

Description

There are several issues that are known to be present in the solc 0.8.13, with some being introduced in this version.

Proof of Issue

File name: hardhat.config.ts

Line number: 13

```
module.exports = {
  solidity: {
    version: '0.8.13',
    settings: {
      optimizer: {
        enabled: true,
        runs: 999999,
      },
    },
  },
```

Severity and Impact Summary

Solc `0.8.13` is affected by the following issues

- SOL-2022-2: NestedCallataArrayAbiReencodingSizeValidation (very low)
- SOL-2022-3: DataLocationChangeInInternalOverride (very low)
- SOL-2022-4: InlineAssemblyMemorySideEffects (medium)
- SOL-2022-5: DirtyBytesArrayToStorage (low)

Recommendation

It is recommended to use the version of compiler not affected by the medium issue (SOL-2022-4) by either upgrading it to “0.8.15” or downgrading it to a safe version. Please note that “0.8.15” is the most recent version at the moment and it may not be fully supported by different tools yet.

References

- https://docs.soliditylang.org/en/latest/bugs.html

INCOMPLETE BUILD INSTRUCTIONS

Finding ID: FYEO-AB-02
Severity: **Informational**
Status: **Open**

Description

The build instructions are incomplete and some dependencies are missing.

Proof of Issue

File name: README.md

Line number: 13

```
### Build

- `npm run compile`
- `npm run test`
```

Severity and Impact Summary

The complete build instruction will simplify assembly in a new environment.

The command should be `npm run build` instead of `npm run compile`

Missing package `npm i --save-dev ts-node`

Missing package `npm i --save-dev @types/mocha`

Recommendation

It is recommended to add missing dependencies and update build instruction.

PUBLIC VISIBILITY IS SET FOR FUNCTIONS THAT ARE NOT CALLED INTERNALLY

Finding ID: FYEO-AB-03
Severity: **Informational**
Status: **Remediated**

Description

Public visibility is used for functions that should be accessible from other contracts, via transactions, and from the current contract. Functions that are not meant to be called internally should have external visibility.

Proof of Issue

File name: contracts/Inbox.sol

Line number: 68

```
    function initialize(uint32 _remoteDomain, address _validatorManager)
        public
        initializer
```

File name: contracts/Outbox.sol

Line number: 89

```
    function initialize(address _validatorManager) public initializer
```

Severity and Impact Summary

External functions may be more GAS efficient, especially with functions that receive a lot of data in parameters.

Recommendation

It is recommended to set external visibility for functions that are not called internally.

References

- https://docs.soliditylang.org/en/v0.7.4/contracts.html?highlight=external#visibility-and-getters

Our Process

Methodology

FYEO Inc. uses the following high-level methodology when approaching engagements. They are broken up into the following phases.

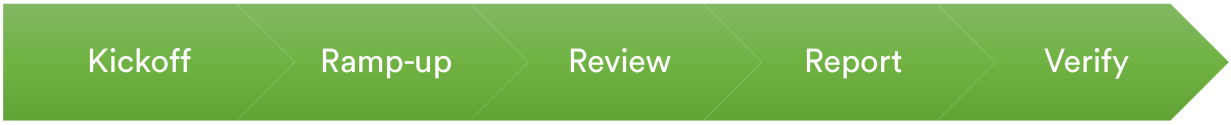

Figure 2: Methodology Flow

Kickoff

The project is kicked off as the sales process has concluded. We typically set up a kickoff meeting where project stakeholders are gathered to discuss the project as well as the responsibilities of participants. During this meeting we verify the scope of the engagement and discuss the project activities. It's an opportunity for both sides to ask questions and get to know each other. By the end of the kickoff there is an understanding of the following:

- Designated points of contact
- Communication methods and frequency
- Shared documentation
- Code and/or any other artifacts necessary for project success
- Follow-up meeting schedule, such as a technical walkthrough
- Understanding of timeline and duration

Ramp-up

Ramp-up consists of the activities necessary to gain proficiency on the project. This can include the steps needed for familiarity with the codebase or technological innovation utilized. This may include, but is not limited to:

- Reviewing previous work in the area including academic papers
- Reviewing programming language constructs for specific languages
- Researching common flaws and recent technological advancements

Review

The review phase is where most of the work on the engagement is completed. This is the phase where we analyze the project for flaws and issues that impact the security posture. Depending on the project this may include an analysis of the architecture, a review of the code, and a specification matching to match the architecture to the implemented code.

In this code audit, we performed the following tasks:

1. Security analysis and architecture review of the original protocol
2. Review of the code written for the project
3. Compliance of the code with the provided technical documentation

The review for this project was performed using manual methods and utilizing the experience of the reviewer. No dynamic testing was performed, only the use of custom-built scripts and tools were used to assist the reviewer during the testing. We discuss our methodology in more detail in the following sections.

Code Safety

We analyzed the provided code, checking for issues related to the following categories:

- General code safety and susceptibility to known issues
- Poor coding practices and unsafe behavior
- Leakage of secrets or other sensitive data through memory mismanagement
- Susceptibility to misuse and system errors
- Error management and logging

This list is general and not comprehensive, meant only to give an understanding of the issues we are looking for.

Technical Specification Matching

We analyzed the provided documentation and checked that the code matches the specification. We checked for things such as:

- Proper implementation of the documented protocol phases
- Proper error handling
- Adherence to the protocol logical description

Reporting

FYEO Inc. delivers a draft report that contains an executive summary, technical details, and observations about the project.

The executive summary contains an overview of the engagement including the number of findings as well as a statement about our general risk assessment of the project. We may conclude that the overall risk is low but depending on what was assessed we may conclude that more scrutiny of the project is needed.

We report security issues identified, as well as informational findings for improvement, categorized by the following labels:

- Critical
- High
- Medium
- Low
- Informational

The technical details are aimed more at developers, describing the issues, the severity ranking and recommendations for mitigation.

As we perform the audit, we may identify issues that aren't security related, but are general best practices and steps that can be taken to lower the attack surface of the project. We will call those out as we encounter them and as time permits.

As an optional step, we can agree on the creation of a public report that can be shared and distributed with a larger audience.

Verify

After the preliminary findings have been delivered, this could be in the form of the approved communication channel or delivery of the draft report, we will verify any fixes within a window of time specified in the project. After the fixes have been verified, we will change the status of the finding in the report from open to remediated.

The output of this phase will be a final report with any mitigated findings noted.

Additional Note

It is important to note that, although we did our best in our analysis, no code audit or assessment is a guarantee of the absence of flaws. Our effort was constrained by resource and time limits along with the scope of the agreement.

While assessing the severity of the findings, we considered the impact, ease of exploitability, and the probability of attack. This is a solid baseline for severity determination.

THE CLASSIFICATION OF VULNERABILITIES

Security vulnerabilities and areas for improvement are weighted into one of several categories using, but is not limited to, the criteria listed below:

Critical – vulnerability will lead to a loss of protected assets

- This is a vulnerability that would lead to immediate loss of protected assets
- The complexity to exploit is low
- The probability of exploit is high

High - vulnerability has potential to lead to a loss of protected assets

- All discrepancies found where there is a security claim made in the documentation that cannot be found in the code
- All mismatches from the stated and actual functionality
- Unprotected key material
- Weak encryption of keys
- Badly generated key materials
- Txn signatures not verified
- Spending of funds through logic errors
- Calculation errors overflows and underflows

Medium - vulnerability hampers the uptime of the system or can lead to other problems

- Insecure calls to third party libraries
- Use of untested or nonstandard or non-peer-reviewed crypto functions
- Program crashes, leaves core dumps or writes sensitive data to log files

Low – vulnerability has a security impact but does not directly affect the protected assets

- Overly complex functions
- Unchecked return values from 3rd party libraries that could alter the execution flow

Informational

- General recommendations