F Y E O

Security Code Review of Censo Wallet Integration

Censo

January 2024
Version 1.0

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

Security Level
Public

Table of Contents

Executive Summary....2
- Overview....2
- Key Findings....2
- Scope and Rules of Engagement....2

Technical Analyses and Findings....4
- Findings....5
- Technical Analysis....5
- Conclusion....5

Technical Findings....6
- General Observations....6
- Pin dependencies to specific versions....7
- Signature is logged to the console....8

Our Process....9
- Methodology....9
- Kickoff....9
- Ramp-up....9
- Review....10
- Code Safety....10
- Technical Specification Matching....10
- Reporting....11
- Verify....11

Additional Note....11

The Classification of vulnerabilities....12

Executive Summary

Overview

Censo engaged FYEO Inc. to perform a Security Code Review of Censo Wallet Integration.

The assessment was conducted remotely by the FYEO Security Team. Testing took place on January 12 - January 17, 2024, 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 the risk they pose:

- FYEO-CENSO-01 – Pin dependencies to specific versions
- FYEO-CENSO-02 – Signature is logged to the console

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 Code Review of Censo Wallet Integration. 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 via 3 repositories:

github.com/Censo-Inc/censo-wallet-integration-android 0323c0211b13ab081eb33c4a6db4ac0f0223157d

github.com/Censo-Inc/censo-wallet-integration-ios f9ff7bfffb7c418e0da3605c992be024ad3135cd

github.com/Censo-Inc/censo-wallet-integration b3cca353eaed862115ffd04768c411be99637964

- Remediated SHA: 2b56a38aea6882d4d6480b45f9be0e51779d2e1f

Files included in the code review

censo-wallet-integration/
└── src/
  ├── index.ts
  └── types.d.ts
 	
Android
└── main/java/co/censo/walletintegration
  ├── ApiService.kt
  ├── Base58EncodedPublicKey.kt
  ├── Base64EncodedData.kt
  ├── CensoWalletIntegration.kt
  ├── ECIESManager.kt
  ├── ECPublicKeyExtensions.kt
  ├── Model.kt
  ├── Session.kt
  └── Utils.kt
 	
iOS
└── CensoSDK
  ├── Base58.swift
  ├── CensoSDK.swift
  ├── Data+Hex.swift
  ├── DateFormat.swift
  ├── EncryptionKey.swift
  ├── Error.swift
  ├── Model.swift
  ├── Session.swift
  ├── SigningKey.swift
  └── ValueWrappers.swift

Table 1: Scope

Technical Analyses and Findings

During the Security Code Review of Censo Wallet Integration, we discovered:

- 1 finding with MEDIUM severity rating.
- 1 finding with LOW severity rating.

The following chart displays the findings by severity.

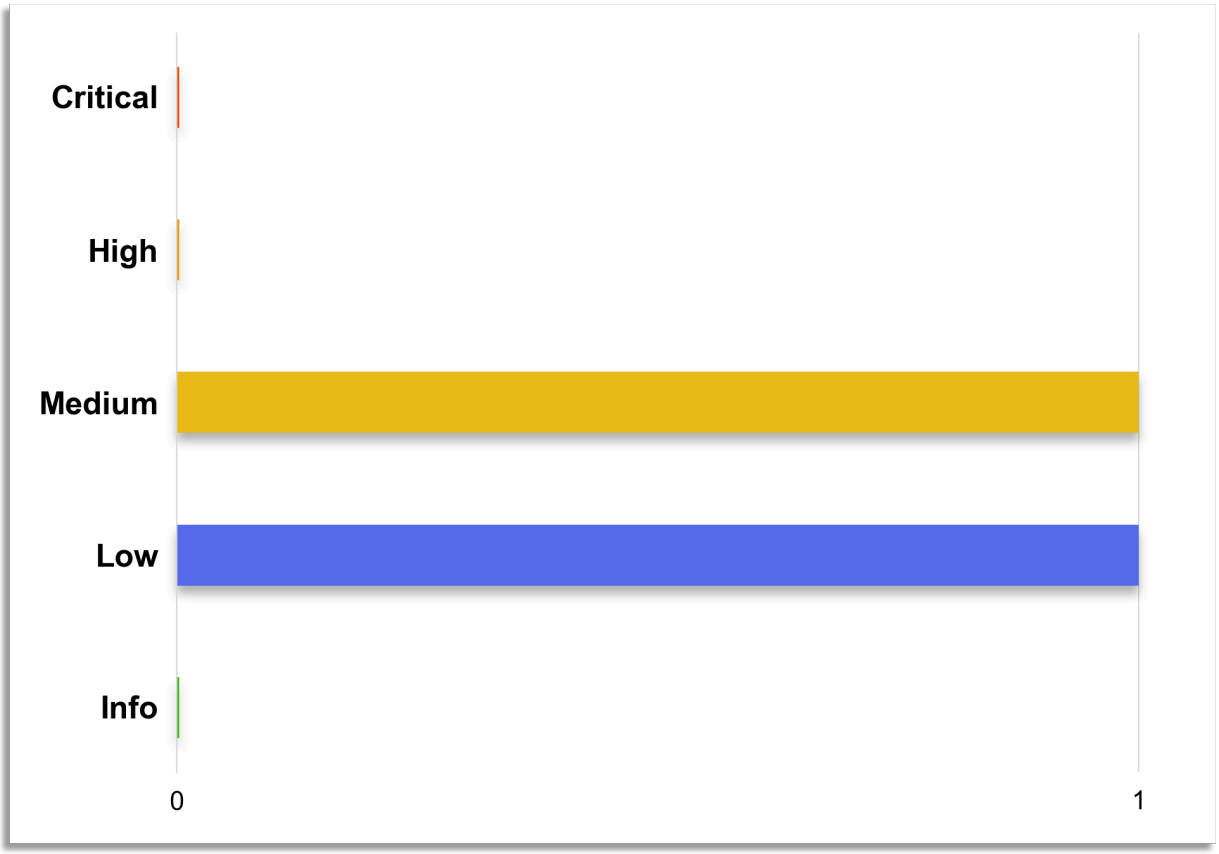

Figure 1: Findings by Severity

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-CENSO-01	**Medium**	Pin dependencies to specific versions
FYEO-CENSO-02	**Low**	Signature is logged to the console

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.

Conclusion

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

The code base displays a strong foundation with a multitude of positive aspects, it is evident that the team has invested significant effort in creating a well-organized code base that is easy to follow.

The comments provided are sparse and could be more comprehensive in elucidating the rationale behind specific design choices, algorithmic decisions, and complex sections of code. Enhancing the comments would not only facilitate a quicker understanding of the codebase for future developers but also ensure maintainability and ultimately aid in the long-term maintainability of the code base.

Overall, the team's efforts in creating a well-organized code base are commendable. Enhancing the in-code documentation will further improve the project's quality and maintainability.

Pin dependencies to specific versions

Finding ID: FYEO-CENSO-01
Severity: **Medium**
Status: **Remediated**

Description

The dependencies are not pinned to specific versions, weakening the security of this app.

Proof of Issue

File name: package.json
Line number: 8

```
"dependencies": {
  "axios": "^1.6.2",
  "bip39": "^3.1.0",
  "bs58": "^5.0.0",
  "crypto-browserify": "^3.12.0",
  "js-crypto-ec": "^1.0.7",
  "js-crypto-key-utils": "^1.0.7",
  "js-sha256": "^0.10.1",
  "yarn": "^1.22.21"
},
```

Severity and Impact Summary

It is possible that a bad actor manages to compromise one of the dependencies and push a malicious update.

Recommendation

Pin dependencies to specific version and update when required.

Signature is logged to the console

Finding ID: FYEO-CENSO-02
Severity: **Low**
Status: **Remediated**

Description

The code logs the cryptographic signature to the console.

Proof of Issue

File name: src/index.ts
Line number: 121

```
console.log("Could not convert signature from DER to P1363 format", derSignature)
```

Severity and Impact Summary

Signatures should be handled carefully.

Recommendation

Do not log this data to the console.

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