FYEO

Censo Android & iOS

Security Review Update: Jan 29, 2024

Reviewer: balthasar@gofyeo.com

Censo App Security Review Update

New security issues, 1

After the development team implemented the latest updates, FYEO conducted a review of the modifications. The primary goal of this evaluation was to ensure the continued robustness of the app's security features, safeguarding user data and maintaining the overall integrity of the applications.

General Updates:

The most recent update to the iOS and Android Apps introduces several new features and enhancements to improve user security and overall experience. Notable changes include the addition of a login recovery feature, allowing users to regain access through collaboration with their designated "Approvers”, fortified by biometric authentication and password verification.

The introduction of timelock functionality provides users with another security feature by giving them time to act in case of adverse events.

The user interface has undergone updates, offering a more intuitive experience. Improved explanations within the app guide users effectively. Users can also view optional explanations should they desire to gain a deeper understanding. An owner selection screen has been added for iOS. The Android UI received a new WelcomeScreen and PhraseImportScreen. A maintenance mode overlay ensures a smoother experience during maintenance periods, effectively communicating downtime while maintaining a professional appearance.

The update also includes the introduction of a new API health endpoint for performance monitoring. A seamless migration process from version 2 to version 3 ensures users can transition without data loss or disruptions.

Users can now label the people they are helping secure seed phrases for, making it easier to help multiple people with clarity.

Users with diverse crypto portfolios wishing to secure several seed phrases will need to upgrade to a paid version. Additionally, app code redemption has been introduced to simplify the onboarding process.

Another update for iOS involves swapping Raygun for Sentry for error tracking and diagnostics.

Collectively, these updates contribute to a more secure, user-friendly, and feature-rich experience within the iOS and Android Apps, empowering users to manage and recover their seed phrases with confidence.

Specific Security Changes:

During the course of the review, an observation was made regarding the TOTP (Time-based One-Time Password) generator, which was found to lack the use of a secure random number generator. It is noteworthy that the development team has already rectified this issue, ensuring the incorporation of a secure random generator in the TOTP code generation process.

Commit Hash Reference:

For transparency and reference, the security review was conducted on the specific commit hashes for both the iOS and Android repositories. The commit hashes for the reviewed versions are as follows:

iOS: f02824554f53efccde6fec9ad13c6ddfc7a65b7f
Android: abc233439688d194cc8752ebed4a1e2d1622f520

Conclusion:

In conclusion, the security aspects of both Censo apps remain robust and unaffected by the recent updates. Users can confidently interact with the application, assured that their seed phrases and stored data are well-protected. The commitment to security exhibited by the development team is commendable, and we appreciate the ongoing efforts to prioritize the safeguarding of user information.