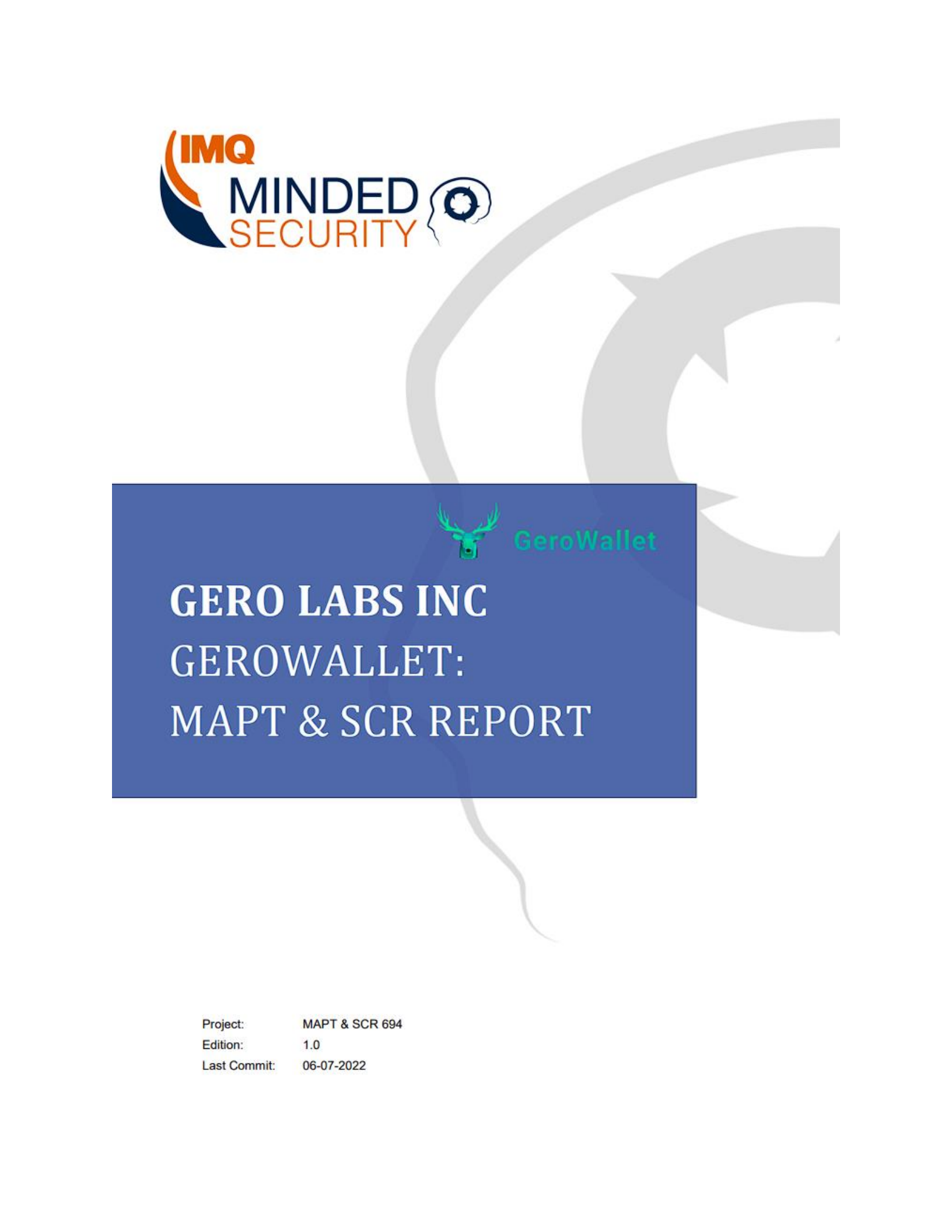

GeroWallet

GERO LABS INC
GEROWALLET:
MAPT & SCR REPORT

Project:	MAPT & SCR 694
Edition:	1.0
Last Commit:	06-07-2022

Contents

Introduction

The goal of a Mobile Application Penetration Test (MAPT) assessment is to simulate all possible attack scenarios towards a mobile application. The intent is to find, and fix, weaknesses before the deployment of the mobile application. The assessment provides an evaluation of the overall security of the mobile application by identifying vulnerabilities and estimating the likelihood of such vulnerabilities being exploited by a real attacker. The goal of a Source Code Review (SCR) activity is to analyze the security of a mobile application by considering its source code.

This activity is generally carried out manually by consultants, however, in certain scenarios, it can be supported by the use of semi-automatic tools. During an SCR, consultants analyze the source code of the mobile application in search of vulnerabilities. The source code analysis provides detailed information on the actual implementation of the mobile application that consequently allows the identification of vulnerabilities. Gero Labs Inc asked IMQ Minded Security to perform a Mobile Application Penetration Test (MAPT) and a Source Code Review (SCR) of the mobile application GeroWallet.

The mobile applications in scope for this activity were provided by Gero Labs Inc through the Play Store for the Android application and trough TestFlight for the iOS application. The source code of the mobile application and of the GeroWallet API was retrieved from the GitLab project using the “develop” branch as requested from Gero Labs Inc. Following the MD5 hash of the source code retrieved from GitLab: 405c2ded4331231a155f26c8b32bd9a1 GERO-SERVER-develop.zip The MAPT and SCR activity took place from IMQ Minded Security offices during the following dates:

- 05-23-2022 – Start of the activity
- 06-07-2022 – End of the activity

Limitations

It is worth considering that since the activity has been conducted on Production environment no extensive tests have been conducted against the target "api.moonpay.com" since it does not belong to the owner of the GeroWallet application. The aforementioned target is used by the application in order to buy ADA coins. Finally, please note that as requested from Gero Labs Inc the swap functionality has not been tested since it was not implemented in the provided application and will be tested in a further activity.

Executive Summary

At the time of the analysis, IMQ Minded Security did not find any vulnerabilities that could directly and easily impact or undermine the safety of the user’s funds. At the time of testing the GeroWallet application, only specific hooking attacks could impact on the user funds. However, these kind of attacks request a malicious and privileged application to be already installed within the victim device in order to change the GeroWallet application behavior. For the most part the findings described below are recommended as a best practice to strengthen the resiliency of the application against reverse engineer and runtime modifications.

Results

The assessment activity has found 15 different types of vulnerabilities. For each type of vulnerability, it was performed a technical impact analysis, which has pointed out:

- A number of 2 High risk vulnerabilities
- A number of 8 Medium risk vulnerabilities
- A number of 5 Low risk vulnerabilities

High Risk Vulnerabilities

Missing Runtime Integrity Protection [Android][iOS]

The application does not implement any integrity check to prevent arbitrary modification to the application behavior at run-time. The lack of this type of controls makes easier for a malicious user to control the behavior of the mobile application

GeroWallet Response: Improving the resiliency against reverse engineer techniques is desirable and will be implemented in subsequent application versions. However, these kind of attacks request a malicious and privileged application to be already installed within the victim device in order to change the GeroWallet application behavior.

Missing Root and Jailbreak Detection [Android][iOS]

During the analysis it has been found that both the applications do not implement any check in order to detect the execution on rooted or jailbroken devices. Giving the chance to run the application on rooted or jailbroken devices could permit reverse engineering attempts and expose the application to various form of data interception.

GeroWallet Response: Improving the resiliency against reverse engineer techniques is desirable and will be implemented in subsequent application versions. However, this risk does not directly undermine user's funds safety since it is not a direct exploit but a sign of a less secure device which could allow subsequent attacks.

Medium Risk Vulnerabilities

Missing Profile Risk Assessment [Android][iOS]

Requiring users to set device-level passcode is a simple feature that creates a significant obstacle for an attacker. If the passcode is not set, anyone can unlock the phone and steal the wallet data or even access the Keychain/Keystore.

GeroWallet Response: Finding the right balance between security and useability is always a challenge. We believe is best not to be intrusive and let the user decide how they want to protect their mobile in general. As a compensating control the GeroWallet application required a password at login and whenever any transactions will take place.

SSL Pinning Not Implemented [Android][iOS]

During the activity it has been found that both the applications do not implement SSL Certificate Pinning, thus they could be involved in Man-in-theMiddle (MitM) attacks if malicious Certificate

Authority (CA) certificates were installed onto the device. Upon installing a malicious CA certificate on the device, it is possible to intercept the traffic generated by the application through an HTTPS Proxy.

GeroWallet Response: SSL Pinning is something we can implement is subsequent versions. The compensating control is that once a TX is signed even if it is somehow exposed to a malicious actor in transit it cannot be altered on manipulated in any way. The malicious actor would need the user's private key to make any acceptable by the network changes.

Secrets in Source Code [Android][iOS][Server]

During the activity it has been found that some secrets are hardcoded in the source code of the application, such as the "projectId" used to authenticate against the Blockfrost services, the password used to sign the MoonPay url and other access tokens.

GeroWallet Response: Although hardcoded secrets are not a best practice, the MoonPay ID and BlockFrost ID do not affect the end user in any way. Going forward, the team will remove these hardcoded values to adhere with best practices.

Application Screenshot Allowed [Android][iOS]

During the activity it has been found that both the applications allow manual screenshots. This possibility may pose a security risk because sensitive data may be exposed if the user deliberately screenshots the application while sensitive data is displayed. A malicious application that is running on the device and able to continuously capture the screen may also expose data. Specifically, it has been found that both the applications allow manual screenshot within the password creation and secret backup phrase windows.

GeroWallet Response: Planned to be remediated with next version update in January 2023

Missing File Integrity Check [Android][iOS]

It has been found that the application does not implement any check in order to detect the integrity of its files. The risk associated to this missing verification is that an attacker could create a malicious version of production application disabling the security checks implemented on it or enabling the debug mode in order to reverse engineer the application.

GeroWallet Response: Improving the resiliency against reverse engineer techniques is desirable and will be implemented in subsequent application versions. However, this risk does not directly undermine user's funds safety.

Missing Code Obfuscation [Android][iOS]

During the analysis it has been found that both the applications do not obfuscate their source code sufficiently. An attacker could decompile the applications extracting sensitive data and reverse engineer the applications for further attacks.

GeroWallet Response: Improving the resiliency against reverse engineer techniques is desirable and will be implemented in subsequent application versions. However, an attacker would need to convince the victim to install a malicious application on the device.

Missing Debug Detection [Android][iOS]

the application does not implement any type of detection against debugging mode. Running the application in debug mode could help an attacker to retrieve useful information about how the application works, in order to perform future attacks.

GeroWallet Response: Improving the resiliency against reverse engineer techniques is desirable and will be implemented in subsequent application versions. However, this risk does not directly undermine user's funds safety.

Recent Apps Image Not Obfuscated [Android][iOS]

The Recent Apps is a system-level UI that lists recently accessed activities and tasks. The user can navigate through the list and select a task to resume, or the user can remove a task from the list by swiping it away. If the Recent Apps image contains sensitive data, those could be stolen by an attacker looking at the Recent Apps tab. It has been noticed that both the applications can go on background showing sensitive information such as the password or the secret backup phrase while looking at the Recent Apps tab.

GeroWallet Response: This finding is under investigation and will implemented with subsequent application versions.

Low Risk Vulnerabilities

Default Error Page [Server]

The information present inside a default web page can be used by an attacker in order to perform further targeted attacks against the application. Specifically, it was found that the application shows in some situations, the default AWS ELB error page.

GeroWallet Response: Improving the resiliency against information gathering is desirable and will be implemented in subsequent application versions. However, this risk does not directly undermine user's funds safety.

Misconfigured CORS [Server]

During the assessment, it was found that the application does not properly configure Cross Origin Resource Sharing (CORS) thus allowing an attacker to obtain sensitive information by exploiting an authenticated session established by a victim user.

GeroWallet Response: HTTP methods not in use have been disabled and as compensating control, Cloudflare's WAF is also in place protecting the backend infrastructure.

Strict Transport Security Not Enforced [Server]

The application does not set the HTTP StrictTransport-Security response header to enforce HTTPS communications thus paving the way for possible Man-in-the-Middle attacks.

GeroWallet Response: Strict Transport Security Not Enforced is something we can implement is subsequent versions. The compensating control is that once a TX is signed even if it is somehow exposed

to a malicious actor in transit it cannot be altered on manipulated in any way. The malicious actor would need the user's private key to make any acceptable by the network changes.

TLS Weakness (BEAST) [Server]

It has been found that the remote host is vulnerable to the Browser Exploit Against TLS (BEAST) attack that may allow Man-In-The-Middle (MITM) attacks against TLS in order to silently decrypt and obtain authentication tokens, thereby providing an attacker access to data passed between a web server and the web browser accessing the server.

GeroWallet Response: Disallowing week ciphers is something we can implement is subsequent versions. The compensating control is that once a TX is signed even if it is somehow exposed to a malicious actor in transit it cannot be altered on manipulated in any way. The malicious actor would need the user's private key to make any acceptable by the network changes.

Weak TLS Versions Supported [Server]

It was found that the web server supports some deprecated TLS protocol versions. A Man-in-the-Middle attacker could exploit this weakness to decrypt the traffic transmitted between his victim and the web server.

GeroWallet Response: Disallowing week ciphers is something we can implement is subsequent versions. The compensating control is that once a TX is signed even if it is somehow exposed to a malicious actor in transit it cannot be altered on manipulated in any way. The malicious actor would need the user's private key to make any acceptable by the network changes.