Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Management Summary: SolidiFi Wallet Mobile Apps Security Assessment by Cure53, 01.-02.2023

Cure53, Dr.-Ing. M. Heiderich, M. Pedhapati, A. Kahla, B. Casaje

Cure53, an IT security consultancy based in Berlin, conducted a penetration test,source code audit and security assessment of the SolidiFi Wallet mobile applications for Android and iOS. The work was requested by CloudElements in January 2023 and all tests were performed by Cure53 in February 2023, during CW07.

A total of eight days were allocated to reach the coverage expected for this project. The testing conducted for this audit was divided into two distinct Work Packages (WPs) for execution efficiency, as follows:

- **WP1**: Source-code-assisted penetration tests against SolidiFi Wallet Android app
- **WP2**: Source-code-assisted penetration tests against SolidiFi Wallet iOS app

Cure53 was provided with the application builds and sources, test wallets, detailed design documentation, and any alternative means of access required to ensure a smooth review completion. For this purpose, the methodology selected was white-box and a team comprising four senior testers was assigned to the project's preparation, execution, and finalization.

All preparatory actions were completed in January 2023, namely in CW04, to ensure testing could proceed without hindrance or delay. Communications were facilitated via a dedicated, shared Slack channel deployed to combine the workspaces of CloudElements and Cure53, thereby creating an optimal collaborative working environment. All participatory personnel from both parties were invited to partake throughout the test preparations and discussions.

Discussions throughout the test were very good and productive and there were not many questions to be asked. The scope was well prepared and clear, which helped to ensure that there were no significant roadblocks during the test.

A total of *fourteen* findings were identified in this round of testing, seven of which were classified as security vulnerabilities and the remaining seven as general weaknesses with less potential for exploitation. It should be noted that the total number of issues is relatively high, so the overall result after the audit was rather negative. In addition, critical severity levels were found – both relating to the dApp browser - which is not ideal for applications of this nature.

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

However, it should be noted that the audit was immediately followed by a period of fix development by the maintainer team and thorough fix verification by Cure53 based on diffs, PRs and updated builds of the application. Cure53 further positively acknowledged the CloudElements team's due diligence measures to protect users' sensitive information. The use of the React Native SecureStore library to store private keys locally, in an encrypted form, and avoid sending them over the network attests to this commitment.

It is safe to say that all issues have been properly addressed and that the problems highlighted in the original report no longer exist in the currently available version. However, given the purpose of these applications and the results of the audit, it is highly recommended to put a strong emphasis on security and to use the necessary means to do so with each upcoming release, in order to ensure that no damage is done to its users' assets.

In conclusion, this 2023 assessment of the SolidiFi wallet applications for Android and iOS confirms that the mobile application complex under review is now in better shape from a security perspective.

Cure53 would like to thank Ferdi Zoet from the CloudElements team for the excellent project coordination, support, and assistance, both before and during this assignment.