Independent Digital Forensic Analysis of ChatMail® on Renati OS™

Executive Data Extraction Summary of States: Before First Unlock and After First Unlock

Hardware: Pixel 3a device
Android Version: 12
Operating System: Renati
Application: ChatMail

Completed: July 5, 2023
Official Release: August 24, 2023

Applicant

Geoff Green, President & CEO
Myntex Inc.
4511 Glenmore Trail #27,
Calgary, AB T2C 2R9
www.myntex.com
(403) 621-1186

Issued By

Brian Feucht, President & CEO
Unique Wire Inc.
340 NE Evans Street
McMinnville, OR 97128
www.unique-wire.com
(800) 924-3282

Purpose

The client, as the developer of both ChatMail® and Renati™, wanted independent, verifiable testing of their encrypted mobile solution.

The purpose is to provide customers with verifiable assurance that the technology offered is sound and technologically capable of withstanding the latest in physical extraction techniques using both proprietary exploits as well as commercially available forensic tools.

This document summarizes the impartial analysis of the product. Based on the following study.

Scope

1. Utilize all available exploit methods to unlock the device while in:
a) BFU (Before First Unlock) State
b) AFU (After First Unlock) State

2. Extract data off the device while in a:
a) Locked state
b) Unlocked state

3. Attempt decryption, parse, and read extracted data from ChatMail on Renati.

Results

1. Unlock Device
a) No commercially available tool, software or exploit was able to unlock the device in BFU state.
b) No commercially available tool, software or exploit was able to unlock the device in AFU state.

2. Data Extraction
a) No commercially available tool, software or exploit was able to extract any data from the device in a locked state.
b) Using the provided password in an unlocked state, the device still proved to be extremely difficult to obtain an extraction. Only system files and carrier-identifying data were able to be extracted from the device using the password that was provided to us.
c) No user-generated data was able to be extracted.

3. Application Data
a) No user-generated data specifically targeting ChatMail was readable.

Methodology

Gray-box penetration testing was conducted on the device. The certified assessor had been provided with limited knowledge about the security of the product and the IT infrastructure supporting it.

Examiners attempted entry by attempting forensic imaging, password and hash cracking or utilizing side channel exploit attacks. Commercially available digital forensic tools were also employed.

Examiners attempted to find, extract, decrypt, and analyze data from a locked and unlocked state.

Device Overview

To gain access, someone in possession of the device would have to know the password to be authenticated as a normal user. Although messages can be decrypted by an authenticated user, the data cannot be extracted from the device as the USB functionality has been heavily restricted which prevents extraction of data.

Screenshots, Copy & Paste, Fused Location, GPS, NFC, Bluetooth and screen recordings have been removed. The camera is custom and employs encryption. External web browsing and third-party apps are incompatible with the system. Collectively, along with the other disabled features, the device hardening makes it a very strong and capable device for secure communications.

Technical Findings

Data is secure on the device and unauthorized access to the device is currently not possible.

Severity

Risk for exploitation of ChatMail® on Renati™ has been classified as low.

Conclusion

The device was secure against all known exploitation methods as of 7/5/2023.