Yahoo Messenger Android App by Yahoo

Insecure Local Data Storage Vulnerabilities Report

Summary

Introduction

Android provides several options for developers to save persistent application data. The local DB should store data depending on whether the data should be private to your application or accessible to other applications and users. In any case, sensible data always have to be encrypted to avoid privacy violation. Yahoo Messenger keeps user data in a SQLite database, in current scenario, we found below details are stored locally in clear text:

1. List of registered/added buddies in user account
2. List of ignored users
3. **Chat messages in clear text**

This will directly impact the user privacy.

List of detected Vulnerability:

- Insecure Local Data Storage

Vulnerability Description

The Yahoo messenger Android app stores data in a SQLite database locally. Specific Data (chats, friend list etc) stored in this DB are stored in clear text and an adversary that gains access to the device is free to read, delete and edit data.

Ideally databases created in the application will be accessible to any class in the application only, other apps or user cannot access the data directly. But in case of Yahoo messenger data stored in the SQLite DB can be accessed directly without going through the application if the account has root permissions.

References:

OWASP: Insecure Storage

OWASP: Insecure Data Storage

Technical specifications:

Application databases are saved under the following directory:

```
/data/data/com.yahoo.mobile.client.android.im/databases/
```

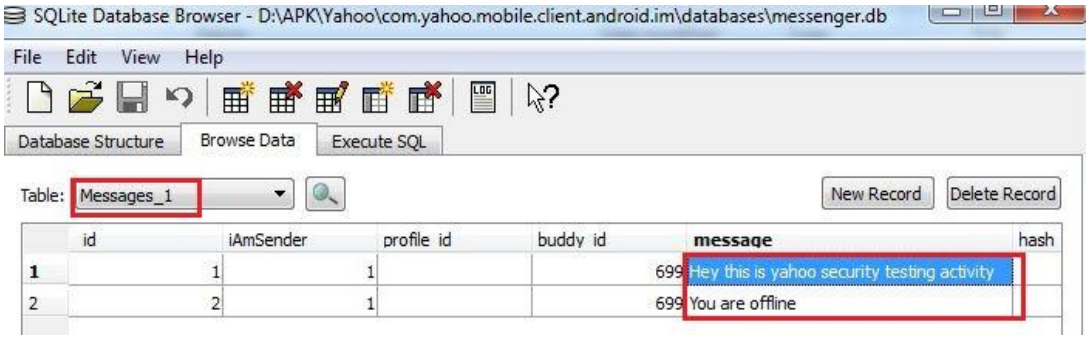
messenger.db holds interesting data like conversations, buddy list, user's account informations. In particular:

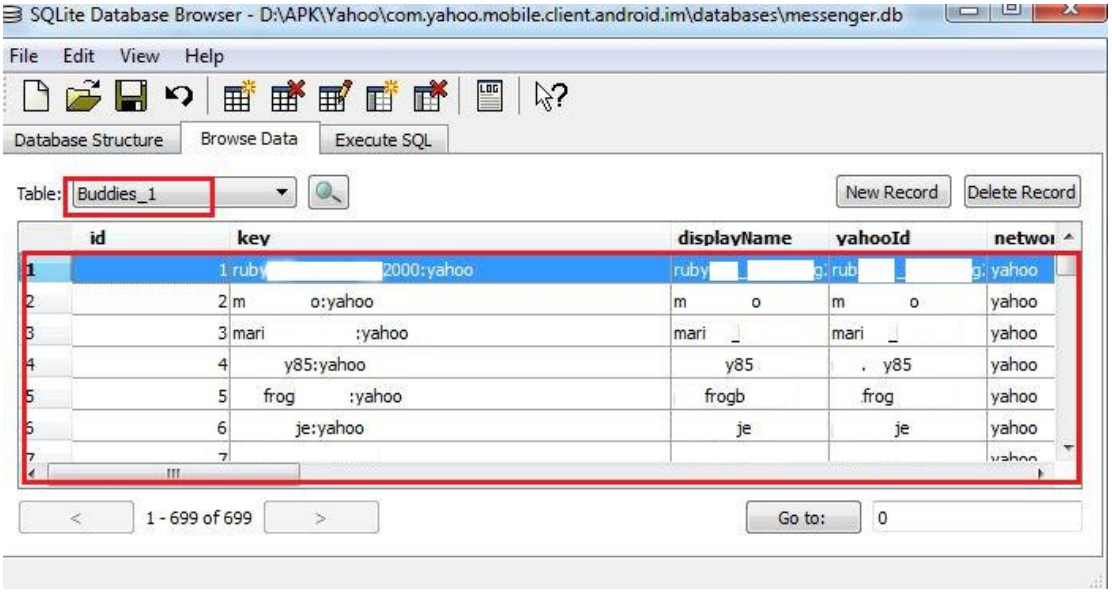
- *Alias, CurrentUser, Session*: contain user's informations;
- *Buddies_1, BuddyAuth_1, BuddyImage_1, GroupMembers_1, Groups_1, IgnoreList_1*: contain informations related to buddies and groups;
- *Messages*: is the db where all conversations are stored, with all related info like who is the sender and timestamp.

share.db holds cookies and session related data, which can be used to impersonate victims and carry out attacks prolonged. In particular:

- *accounts*: contains username, token, YCookie, TCookie e SSLCookie;
- *saredCookies*: contains informations related to shared cookies.

Proof of Concept:





Fix

Insecure Local Data Storage

Encrypt data before insert into the database. As default data in a SQLite are is kept in plain text format. This means that it will always be possible for someone to extract those data, obtaining the .db SQLite file and opening it with a SQLite browser.

Conclusions:

At the moment it is possible for an attacker with physical access to the device or for an application with root privileges to export, read, modify and corrupt the data of conversations.

We haven't found any malware in the wild designed to steal those conversations, maybe due to the lack of interest for cybercriminal.

It's possible to conduct targeted attacks against users in order to retrieve useful information for further social engineering attacks or to make further compromises.

General Information

Reporter	VoidSec Security Team
Authors	Nitin Goplani, Paolo Stagno
Date of contact	22-11-14
Vendor answer	24-11-14
Last vendor reply	24-11-14
Date of public disclosure	05-12-14

Vendor closed the ticket: "*optional security fix that does not represent an immediate threat to safety*". Yahoo will fix the problem in the future.

Common Vulnerability Scoring System 2.0 (CVSS)

Parametro	Punteggio
CVSS Base Score	5.6
CVSS Temporal Score	5.6
CVSS Environmental Score	3.2
Overall CVSS Score	**3.2**

Full CVSS v2 VECTOR:

(AV:L/AC:H/Au:N/C:C/I:C/A:N/E:H/RL:U/RC:C/CDP:N/TD:H/CR:L/IR:L/AR:L)

Informazioni aggiuntive:

Guida CVSS v2

NIST Calculator

Contact Us

VoidSec Security Team | security@voidsec.com | http://voidsec.com | Disclosure Policy