Yahoo Messenger Android App by Yahoo

Insecure Local Data Storage Vulnerabilities Report

Sommario

Introduzione

Android offre agli sviluppatori diverse opzioni per salvare i dati persistenti delle applicazioni. I database locali dovrebbero archiviare i dati in maniera differente, a seconda che i dati siano privati e accessibili solo all'applicazione o all'utente e ad applicazioni esterne. In ogni caso, i dati sensibili dovrebbero sempre essere cifrati per evitare possibili violazioni della privacy. L'applicazione per Android, **Yahoo Messenger,** utilizza un database **SQLite** per memorizzare i dati dell'utente.

Nello scenario attuale, le seguenti informazioni, sono **memorizzati in chiaro**:

1. Lista degli account registrati/aggiunti presenti in lista amici
2. Lista degli account utenti ignorati
3. **Storico delle chat utente**

Le precedenti problematiche impattano direttamente sulla privacy degli utenti.

Lista delle Vulnerabilità riscontrate:

- Insecure Local Data Storage

Descrizione delle vulnerabilità

L'applicazione Yahoo Messenger memorizza i dati in un database SQLite locale. I dati memorizzati all'interno del database: chat, lista amici, ecc. sono memorizzati in chiaro, è pertanto possibile a un malintenzionato che abbia guadagnato l'accesso al dispositivo, leggere, modificare e alterare i dati delle conversazioni.

Idealmente i database creati dall'applicazione sono accessibili solo alle classi dell'applicazione stessa, altre applicazioni o utenti non possono accedere direttamente ai dati.

Nel caso di Yahoo Messenger, i dati archiviati nel database possono essere letti direttamente, senza dover passare "attraverso" l'applicazione se l'account del dispositivo ha permessi di root.

Referenze:

OWASP: Insecure Storage

OWASP: Insecure Data Storage

Specifiche

L'applicazione salva i database nella seguente directory:

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

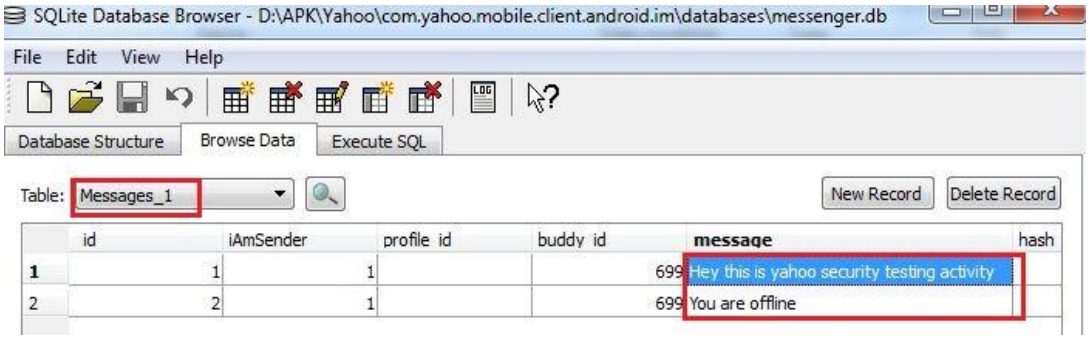
Il database messenger.db contiene i dati d'interesse, quali conversazioni, lista contatti, informazioni relative all'account dell'utente. In particolare le tabelle:

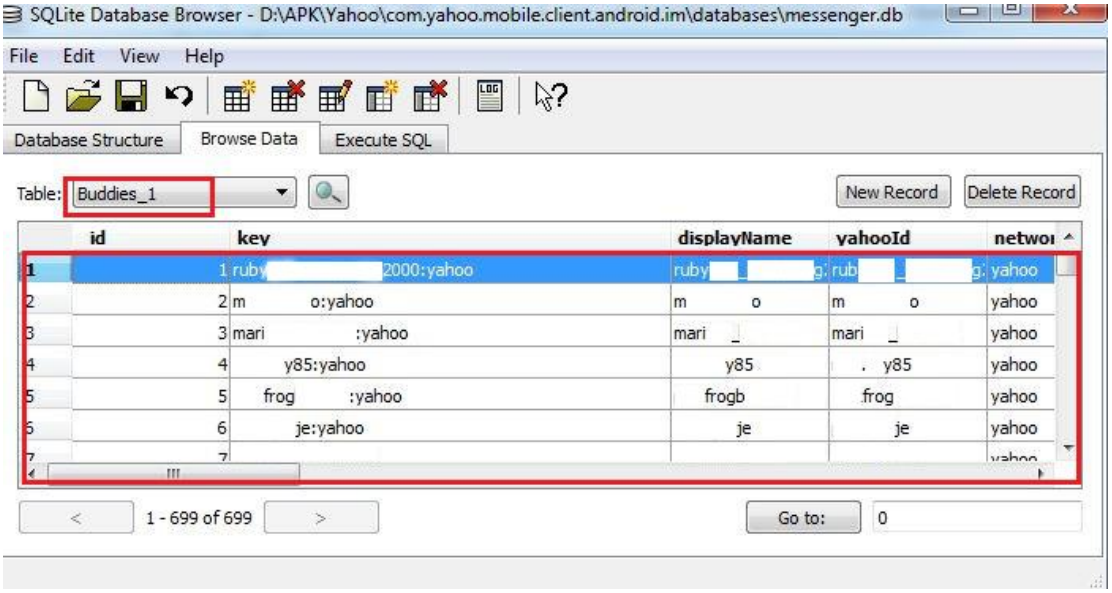
- Alias, CurrentUser, Session: contenenti informazioni relative all'utente;
- Buddies_1, BuddyAuth_1, BuddyImage_1, GroupMembers_1, Groups_1, IgnoreList_1: contenenti informazioni riguardanti i contatti e i gruppi;
- Messages: contiene tutte le conversazioni avvenute con gli utenti, comprese informazioni relative al mittente e timestamp.

Il database share.db contiene tutti i dati relativi ai cookie e al mantenimento delle sessioni, grazie ai quali diventa possibile interpretare la vittima ed effettuare attacchi prolungati nel tempo. In particolare le tabelle:

- accounts: contenente username, token, YCookie, TCookie e SSLCookie;
- saredCookies: contenente informazioni relative ai cookie condivisi con altri servizi.

Proof of Concept:





Fix

Insecure Local Data Storage

Cifare i dati prima di memorizzarli all'interno del database. Di default, i dati di un database SQLite sono mantenuti in plain text, risulta sempre possibile estrarre i dati ottenendo i file .db.

Conclusioni:

Un utente malintenzionato con accesso al dispositivo o a un'applicazione con privilegi di root è in grado di leggere esportare, modificare e alterare i dati delle conversazioni.

Non abbiamo ancora notato malware creato per rubare le conversazioni degli utenti, forse per lo scarso interesse che i cyber criminali nutrono per esse.

E' comunque possibile condurre attacchi mirati nei confronti degli utenti Yahoo Messenger per recuperare informazioni utili ad attacchi di tipo social engineering e portare a termine ulteriori compromissioni ove le conversazioni contengano dati e informazioni sensibili.

Informazioni Generali

Reporter	VoidSec Security Team
Autore	Nitin Goplani
Contatto	22-11-14
Risposta del Vendor	24-11-14
Ultima risposta del Vendor	24-11-14
Data di disclosure pubblica	08-12-14

Il Vendor ha chiuso la segnalazione: "*pratica opzionale che non rappresenta una minaccia immediata alla sicurezza*". Yahoo ha dimostrato interesse a eseguire il fix della problematica in futuro.

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

Contatti

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