Vulnerability in Kaixin001 (开心网) for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
December 31, 2011 at 10:57 AM HKT

Abstract

We found that Kaixin001 1.3.1 and 1.3.3 have a vulnerability that allows a malicious application to access and manipulate user's private information, for example, password (in plaintext!), contacts, personal information, and etc.

1 Application Information

Package Name	com.kaixin001.activity
Full Name	kaixin ("开心网" in Chinese name)
Version	1.3.1 and 1.3.3 (the latest version in Android Market)
Category	Social
Installs	100,000 - 500,000
Average Rating	4.1/5.0 from 1,306 users

CVE Reference	CVE-2011-4866
Vendor	*Kaixin001.com Inc.*., http://www.kaixin001.com/
Vendor Response	

2 Description

Kaixin001 exposes the following content provider in the AndroidManifest.xml file, which is not properly protected, as shown in follows:

```
<provider android:name="com.kaixin001.provider.KaixinContentProvider"
android:authorities="com.kaixin001.provider" />
```

Thus a malicious application on the same device can access and manipulate user's private information, for example, password (in plaintext!), contacts, personal information, and etc., through this content provider.

*** authors with equal contributions**

3 Impact

This vulnerability enables an adversary to access and modify user's private information, such as password (in plaintext!), contacts, personal information, and etc., without being noticed by the user. Such information is supposed to be only accessible to the user having the account and password as shown in Figure 1.

Figure 1: Kaixin001 requires password to log in the system.

However, a malicious application on the same device can manipulate this information without the need to know the account and the password. Figure 2 shows how a malicious application can obtain the user's account and password. It is worth noting that the password is stored in plaintext! Figure 3 illustrates that the user's personal information can be easily fetched by a malicious application.

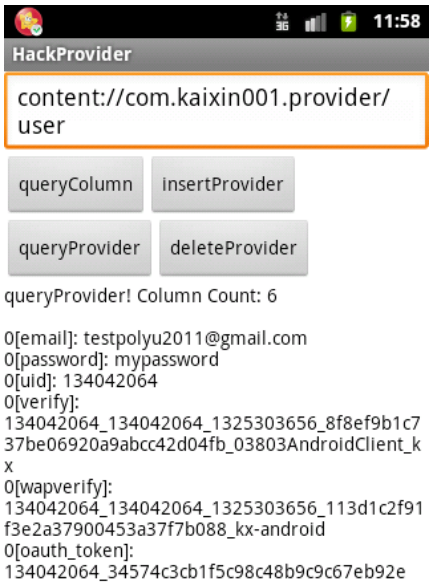

Figure 2: Obtain login information including password in plaintext!

Figure 3: Obtain user's personal information

4 Solution

We are trying our best to contact *Kaixin001.com Inc.* to fix this security issue. Our advice is to set the permission of these application's content providers properly, or avoid exporting these content providers in the AndroidManifest.xml file. Currently, a user could disable the application temporarily and wait for an official update.

5 Technical Description

Among all 9 MiTalk's content providers, 5 of them are vulnerable and sensitive. These 5 content providers have 8 exploitable and sensitive tables in total, as shown in the following table:

Content Provider Authority	Table Name
com.kaixin001.provider	user
com.kaixin001.provider	news
com.kaixin001.provider	friends
com.kaixin001.provider	login
com.kaixin001.provider	newmessage
com.kaixin001.provider	friendsinfo
com.kaixin001.provider	homeinfo

Sample attack codes for manipulate user account:

```
providerUri = Uri.parse("content://com.kaixin001.provider/user")
ContentResolver cr  = this.getContentResolver();
```

```
//Insert
ContentValues values = new ContentValues();
....
outUri = cr.insert(providerUri, values);

//Query
Cursor cursor = cr.query(providerUri, null, null, null, null);

//Delete
int nCount = cr.delete(providerUri, null, null);
```