Vulnerability in MobileQQ (手机 QQ2011) for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
December 29, 2011 at 2:51 PM HKT

Abstract

We found that MobileQQ (手机 QQ2011) has a vulnerability that allows a malicious application to access and manipulate user's private information (e.g., QQ account, friends, messages, and etc.) *protected* by MobileQQ.

1 Application Information

Package Name	com.tencent.mobileqq
Full Name	MobileQQ ("手机 QQ2011" in Chinese name)
Version	2011
Category	Communication
Installs	1,000,000 – 5,000,000
Average Rating	4.1/5.0 from 48,592 users

CVE Reference	CVE-2011-4864
Vendor	*Tencent, Inc.*, http://www.qq.com
Vendor Response	

2 Description

MobileQQ exposes the following content providers in the AndroidManifest.xml file.

```
<provider android:name=".content.ProfileProvider"
android:authorities="qq.profile" />
<provider android:name=".content.FriendListProvider"
android:authorities="qq.friendlist" />
<provider android:name="com.tencent.sc.content.ProfileProvider"
android:process=":sc" android:authorities="qc.profile" />
```

*** authors with equal contributions**

```
<provider android:name="com.tencent.sc.content.FriendFeedProvider"
android:process=":sc" android:authorities="qc.friendfeed" />
<provider android:name="com.tencent.sc.content.RemindFeedProvider"
android:process=":sc" android:authorities="qc.remindfeed" />
<provider android:name="com.tencent.sc.content.MessageRecordProvider"
android:process=":sc" android:authorities="qc.messagerecord" />
```

Since these content providers are not properly protected, a malicious application on the same device can access and manipulate user's private information (e.g., QQ account, friends, messages, and etc.) *protected* by MobileQQ through these content providers.

3 Impact

This vulnerability enables an adversary to access and modify user's private information (e.g., QQ account, friends, messages, 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: MobileQQ 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 QQ account and the password. Figure 2 shows how a malicious application can obtain the user's information by querying the content provider qq.profile. Figure 3 illustrates that the user's friend list, troop list and group information can be fetched through the content provide qq.friendlist. More importantly, the messages sent from a friend can be manipulated as shown in Figure 4.

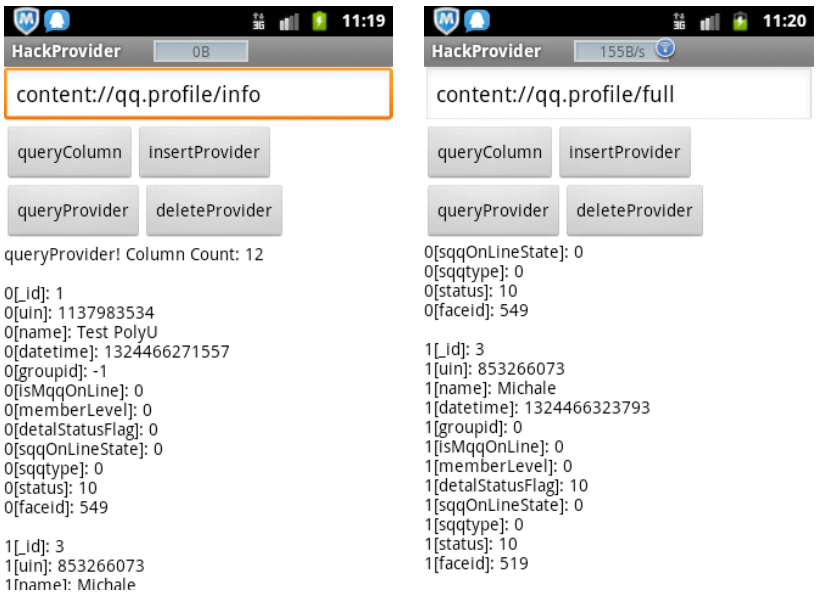

Figure 2: Obtain the user's information

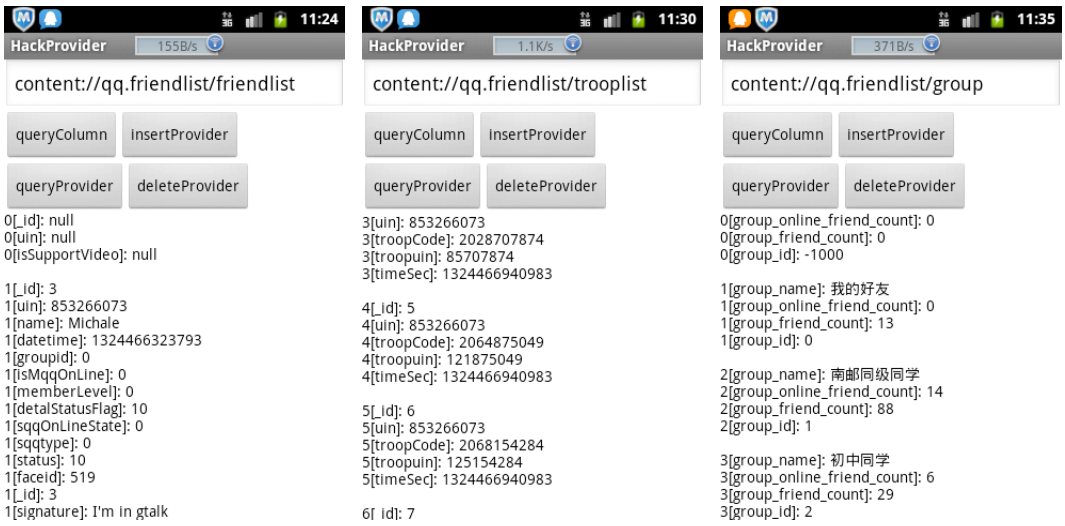

Figure 3: Get the information of the user's friends.

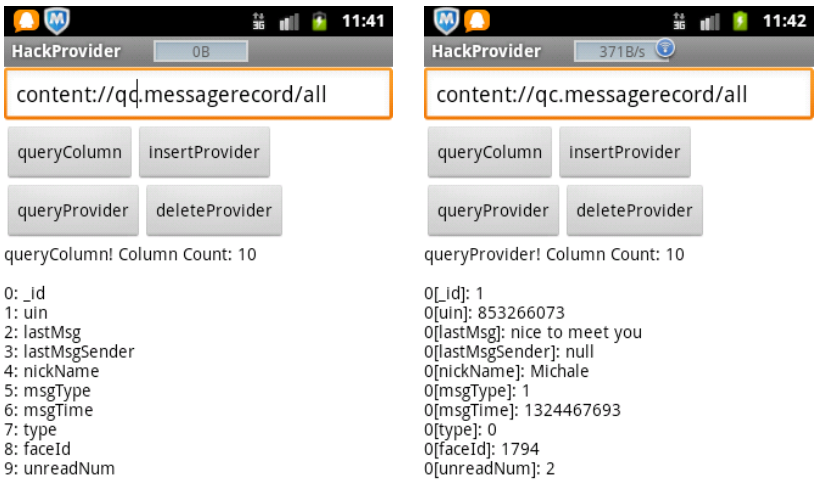

Figure 4: Access the messages

4 Solution

We are trying our best to contact *Tencent 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

The following table shows the names of tables that can be accessed through MobileQQ's content provider. These tables store the user's sensitive information.

Content Provider Authority	Table Name
qq.profile	full
qq.profile	info
qq.friendlist	group
qq.friendlist	friendlist
qq.friendlist	trooplist
qq.friendlist	troopinfo
qq.friendlist	troopname
qc.messagerecord	all
qc.remindfeed	all
qc.friendfeed	all
qc.profile	info
qc.profile	full

Sample attack codes for manipulating message:

```
providerUri = Uri.parse("content://qq.messagerecord/all")
ContentResolver cr  = this.getContentResolver();

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

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

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