Vulnerability in 360 MobileSafe for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
December 13, 2011 PM01:27:23 HKT

Abstract

We found that 360 MobileSafe 2.1.0 and 2.2.0 have 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.qihoo360.mobilesafe
Full Name	360 MobileSafe ("360 手机卫士" in Chinese name)
Version	2.1.0 and 2.2.0 (the latest version in Android Market)
Category	Tools
Installs	500,000 - 1,000,000
Average Rating	4.4/5.0 from 4,506 users

CVE Reference	CVE-2011-4769
Vendor	*Qihoo 360 Technology Co.,Ltd*, http://corp.360.cn/
Vendor Response	None

2 Description

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

```
<provider android:name=".provider.SafeGuardProvider"
android:authorities="com.qihoo360.mobilesafeguard" />
```

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

3 Impact

This vulnerability enables an adversary to access and modify user's all blacklist, sensitive sms, contacts, call logs and etc., without being noticed by user and any privilege. As shown in Figure 1,

*** authors with equal contributions**

a malicious app on the same device can query user's blacklist in 360 MobileSafe, including contact name, blocked type and phone number.

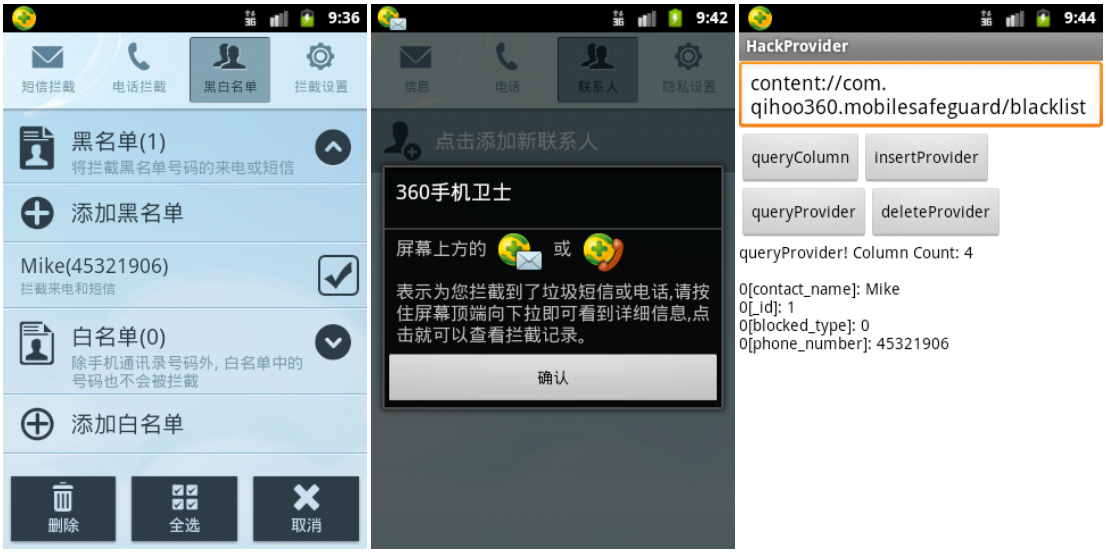

Figure 1: Query blacklist in 360 MobileSafe.

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

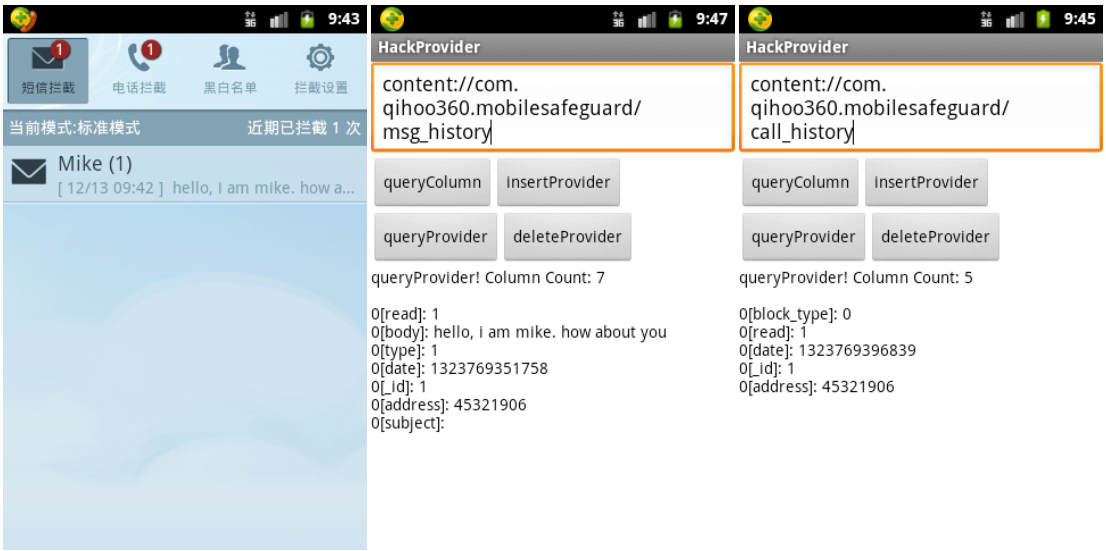

Figure 2: Query block message and call history in 360 MobileSafe.

Moreover, these blacklist and sensitive block contents can also be successfully deleted, as shown in Figure 3. After deleting "blacklist" table, Mike, the previously blacklisted guy, is not blocked by 360 MobileSafe anymore. Thus attacker could launch a data-flow attack to block user's contacts or release blocked contacts without user's attention.

Figure 3: All blacklists could be successfully deleted.

Another major function of 360 MobileSafe is to provide user a private space, as show in Figure 4.

Figure 4: Process of importing sensitive contents into 360 MobileSafe's private space.

However, this private space is not protected properly. As shown in Figure 5 and Figure 6, all sensitive contacts, messages and call logs in 360 MobileSafe's private space could be queried, including contact name, phone number, date, sms body and etc. Although 360 MobileSafe has already encrypted these sensitive attributes in some degree, it's not enough for user's sufficient data security.

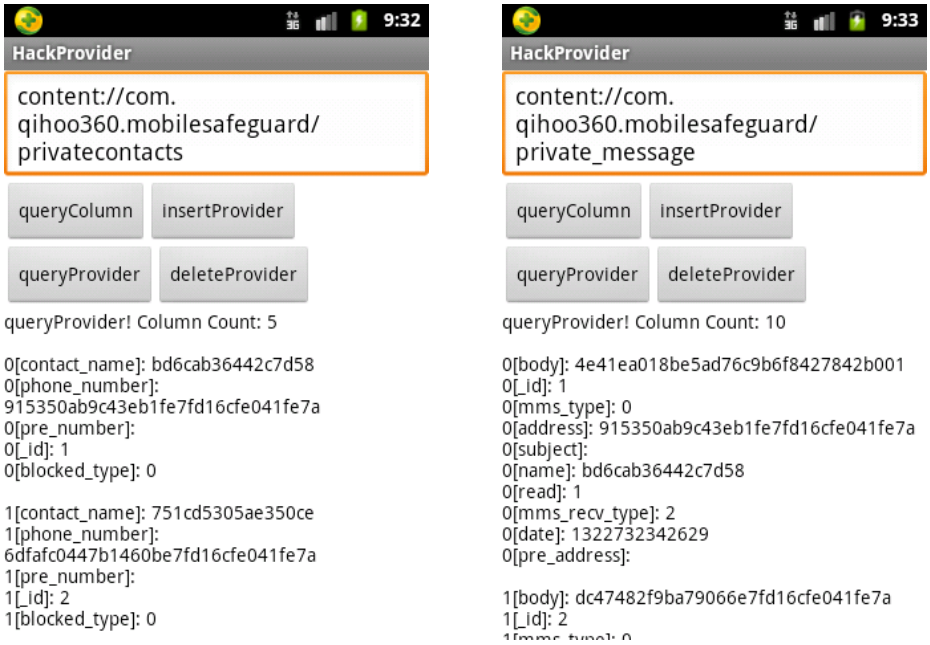

Figure 5: Query sensitive contacts and messages in 360 MobileSafe's private space.

Specially, all these sensitive contents can be deleted and inserted intentionally or unintentionally, as shown in Figure 6.

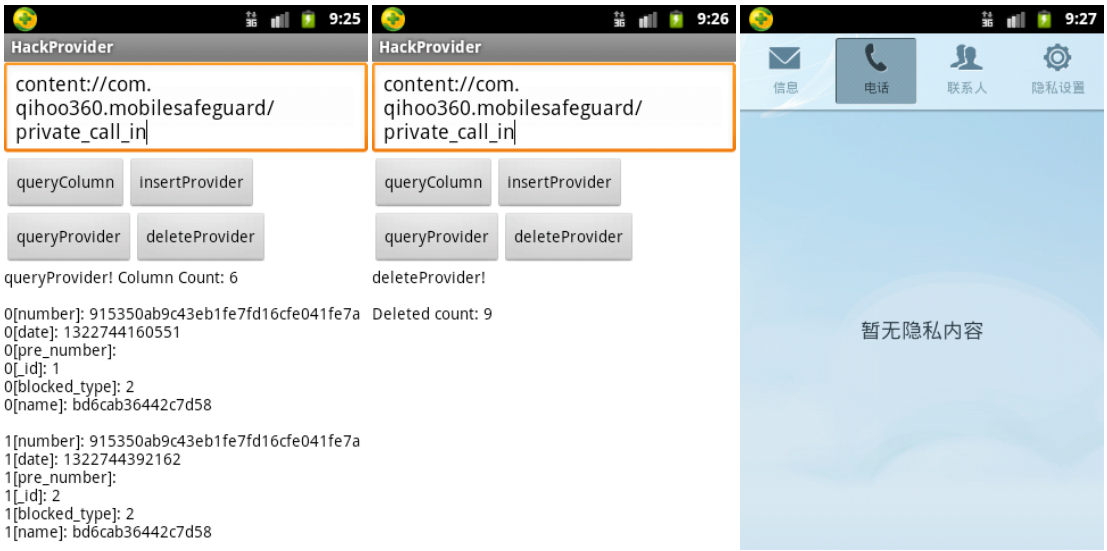

Figure 6: Query and delete sensitive call logs in 360 MobileSafe's private space.

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 MobileSafe only exposes one content provider, "com.qihoo360.mobilesafeguard", it has 12 exploitable and sensitive tables in total, as shown in the following table:

Content Provider Authority	Table Name
com.qihoo360.mobilesafeguard	blacklist
com.qihoo360.mobilesafeguard	call_history
com.qihoo360.mobilesafeguard	ipnouselist
com.qihoo360.mobilesafeguard	msg_history
com.qihoo360.mobilesafeguard	private_call_in
com.qihoo360.mobilesafeguard	private_call_out
com.qihoo360.mobilesafeguard	privatecontacts
com.qihoo360.mobilesafeguard	private_message
com.qihoo360.mobilesafeguard	private_mms_in
com.qihoo360.mobilesafeguard	private_mms_out
com.qihoo360.mobilesafeguard	smartwhite
com.qihoo360.mobilesafeguard	whitelist

Sample attack codes for "blacklist" table in "com.qihoo360.mobilesafeguard":

```
providerUri = Uri.parse("content://com.qihoo360.mobilesafeguard/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);
```