Vulnerability in Voxofon for Android

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

December 2, 2011

Abstract

We found that Voxofon 2.4.3 has a vulnerability that allows a malicious application to access and modify user's sensitive information.

1 Application Information

Package Name	com.voxofon
Full Name	Voxofon - International Calls
Version	2.4.3 (the latest version in Android Market)
Category	Communication
Installs	50,000 - 100,000
Average Rating	4.2/5.0 from 1,012 users

CVE Reference	CVE-2011-4704
Vendor	*Voxofon LLC*, http://www.voxofon.com/
Vendor Response	Null

2 Description

Voxofon exposes the following content provider:"*com.voxofon.provider.VoxofonContentProvider*", through which other applications can access user's contents in Voxofon.

However, this content provider is not properly protected in the AndroidManifest.xml file as shown in follows:

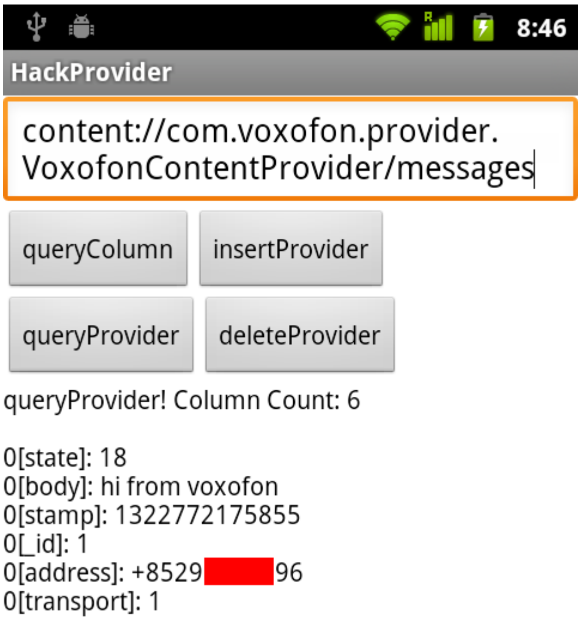
```
<provider android:name="com.voxofon.provider.VoxofonContentProvider"
android:authorities="com.voxofon.provider.VoxofonContentProvider" />
```

Thus a malicious application on the same device can access and modify user's sensitive contents in Voxofon through this content provider.

*** authors with equal contributions**

3 Impact

This vulnerability enables an adversary to access and modify user's sms sent in Voxofon without owning user's Voxofon account. The exposed sensitive information in Voxofon's content provider includes sms content, sending timestamp, recipient's phone number and sending state, as shown in Figure 1. Such sensitive information should only be accessible by applications with granted privilege, and meanwhile with user's acknowledgement.



content://com.voxofon.provider.VoxofonContentProvider/messages

```
queryProvider! Column Count: 6

0[state]: 18
0[body]: hi from voxofon
0[stamp]: 1322772175855
0[_id]: 1
0[address]: +8529[redacted]96
0[transport]: 1
```

Figure 1: The exposed private information in Voxofon's content provider.

4 Solution

We are trying our best to contact *Voxofon LLC* to fix this security issue. Our advice is to set the permission of this application's content provider properly, or just set content provider not exported in the AndroidManifest.xml file. Currently, for a user, just disable the application temporarily and wait for an official update.

5 Technical Description

In the VoxofonContentProvider, it has a table called "messages". Every time user sends a sms from Voxofon's UI, Voxofon would record this sensitive sms information into its "messages" table, including sms content, sending timestamp, recipient's phone number and sending state. However, as VoxofonContentProvider is not well protected in the AndroidManifest.xml file, thus "messages" table is also exposed and accessible by any other applications without privilege.

As a consequence, a malicious application on the same device could query this "messages" table to compromise user’s privacy, or even worse, insert a faked sms (construct recipient as a user’s friend) to phish user’s friends.

Sample attack codes:

```
providerUri =
Uri.parse(“com.voxofon.provider.VoxofonContentProvider/messages”)
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);
```