Vulnerability in MiTalk for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
December 5, 2011

Abstract

We found that MiTalk 1.0, 2.1.280 and 2.1.310 have a vulnerability that allows a malicious application to access and manipulate user's sensitive contacts, sms and etc.

1 Application Information

Package Name	com.xiaomi.channel
Full Name	MiTalk Messenger ("米聊" in Chinese name)
Version	1.0, 2.1.280 and 2.1.310 (the latest version in December 5, 2011)
Category	Social
Installs	100,000 - 500,000
Average Rating	4.3/5.0 from 2,215 users

CVE Reference	CVE-2011-4697
Vendor	*Xiaomi Inc.*, http://www.xiaomi.com/
Vendor Response	Has patched the vulnerability in version 2.1.320 in December 9, 2011

2 Description

MiTalk exposes the following 9 content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

- `<provider android:name=".providers.BuddyProvider" android:authorities="com.xiaomi.channel.providers.BuddyProvider" />`
- `<provider android:name=".providers.SmsContentProvider" android:authorities="com.xiaomi.channel.providers.SmsContentProvider" />`
- `<provider android:name=".providers.OutboxMessageProvider" android:authorities="com.xiaomi.channel.providers.OutboxMessageProvider" />`
- `<provider android:name=".providers.UploadedContactsContentProvider" android:authorities="com.xiaomi.channel.providers.UploadedContactsContentProvider" />`

*** authors with equal contributions**

```
<provider android:name=".providers.MD5CacheContentProvider"
android:authorities="com.xiaomi.channel.providers.MD5CacheContentProvider
" />
<provider android:name=".providers.AttachmentDownloadProvider"
android:authorities="com.xiaomi.channel.providers.AttachmentDownloadProvi
der" />
<provider android:name=".providers.WallProvider"
android:authorities="com.xiaomi.channel.providers.WallProvider" />
<provider android:name=".providers.SystemMessageProvider"
android:authorities="com.xiaomi.channel.providers.SystemMessageProvider"
/>
<provider android:name=".providers.BuddyStatusForPhoneProvider"
android:authorities="com.xiaomi.channel.providers.BuddyStatusForPhoneProv
ider" />
```

Thus a malicious application on the same device can access and manipulate user's sensitive contacts, i.e. buddy and uploaded contacts in this case, and sensitive sms (including attachments) contents through these content providers.

3 Impact

This vulnerability enables an adversary to access and modify user's all sensitive contacts, sms and etc., while without being noticed by the user. The exposed sensitive contacts information includes user's all md5s of local phone's contact numbers, as shown in Figure 1. Attacker could easily first construct a rainbow table containing key-value pairs between common phone numbers and their md5s then compare each md5 with each item in rainbow, thus attacker can get all real phone numbers.

Figure 1: All md5s of local phone's contacts are exposed.

And even worse, all detailed information of buddies in users' MiTalk account all also exposed, including buddies' birthday, username, md5 of email, gender, location, company and school, as shown in Figure 2.

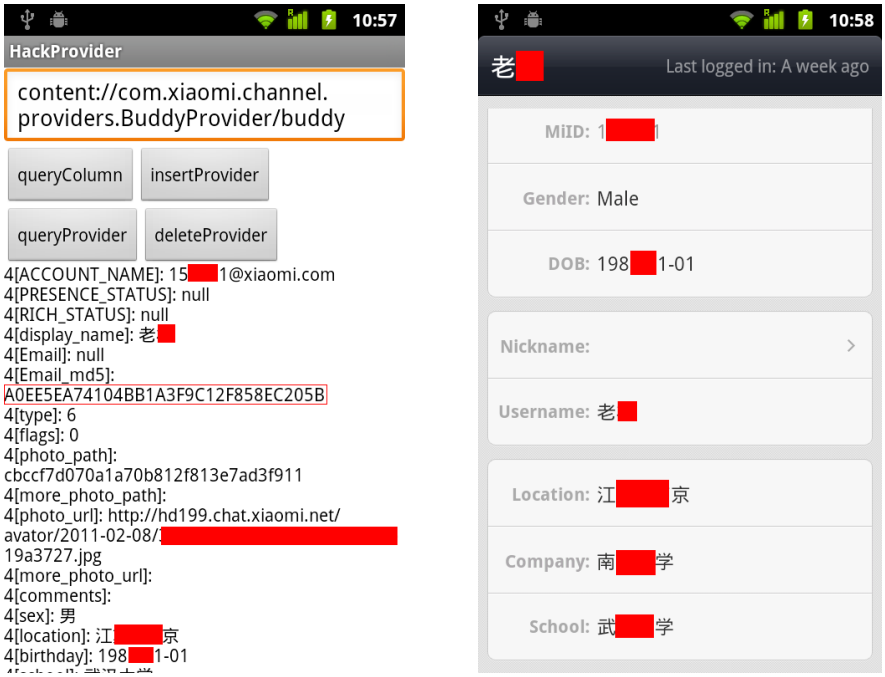

Figure 2: All detailed information of buddies in users' MiTalk account all exposed.

Moreover, all private attributes of user's all sensitive sms are also exposed to public, such as sms content body, sender id, sending time, received time and sender device id, as shown in Figure 3. Meanwhile, in Figure 4, all conversations of sms are also accessible. And all sms published in Wall UI are also exposed, including content and post time, as shown in Figure 5.

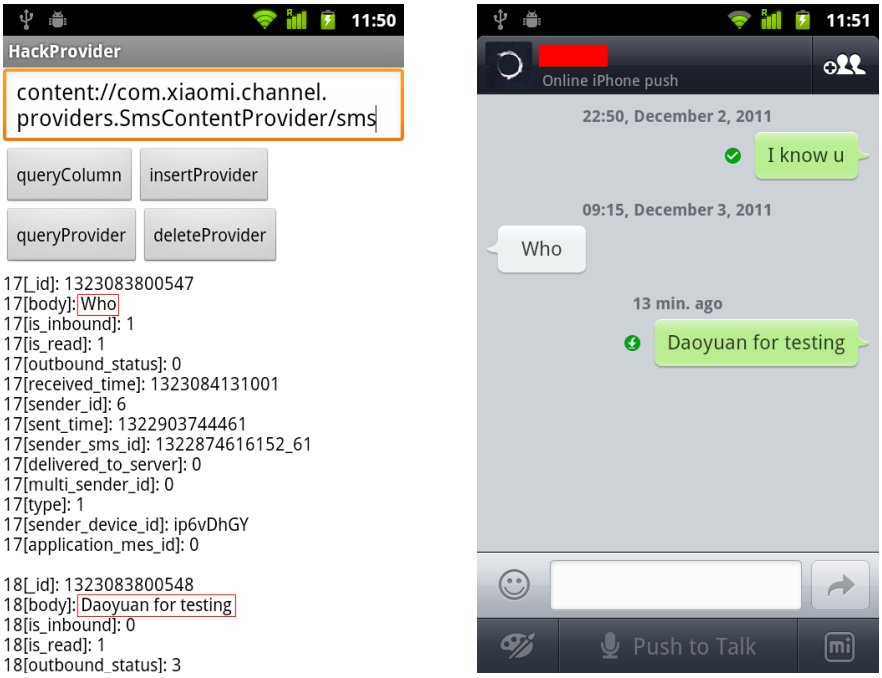

Figure 3: All private attributes of user's all sensitive sms are exposed.

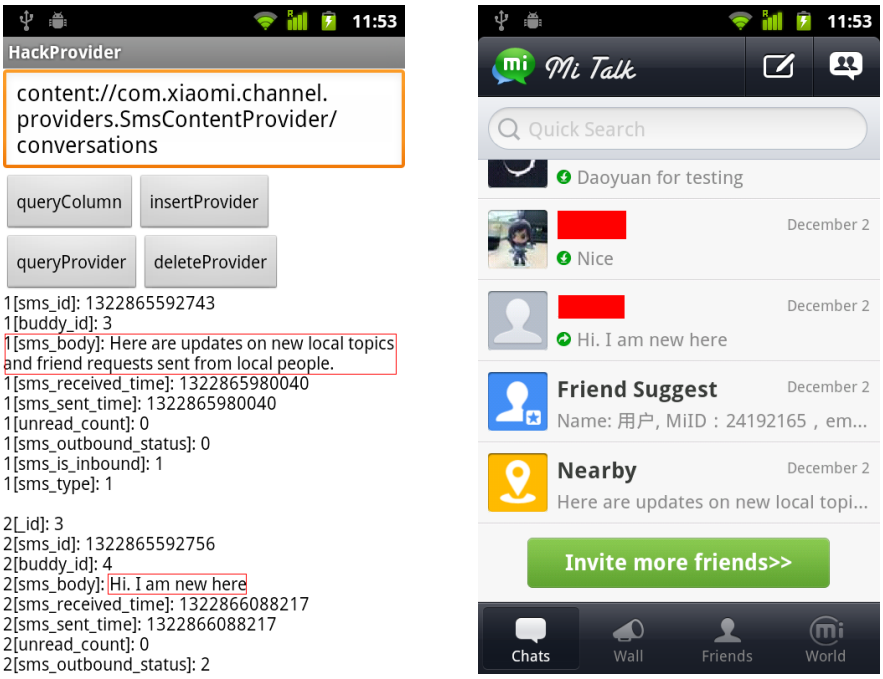

Figure 4: All conversations of sms are accessible.

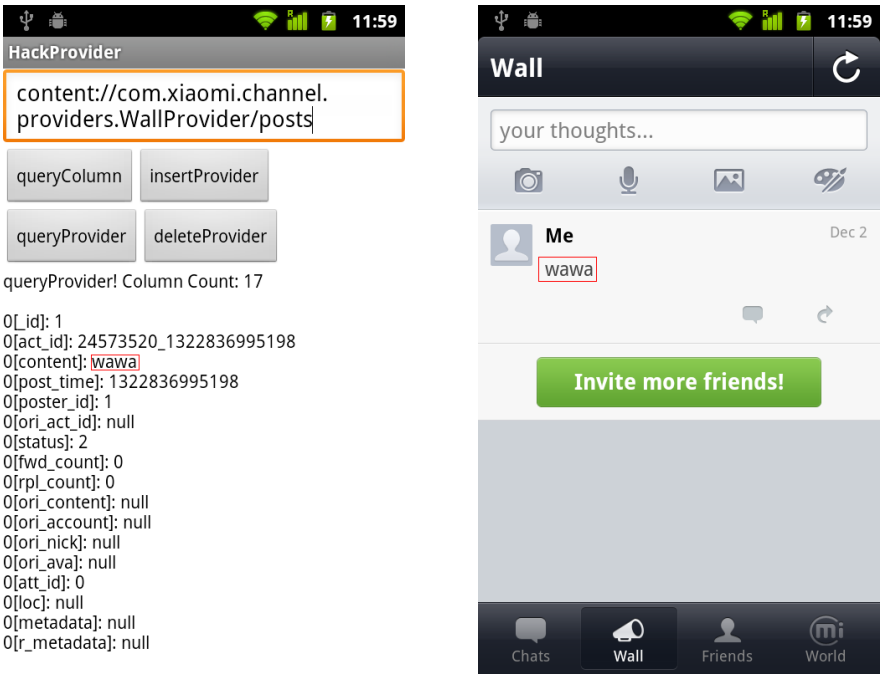

Figure 5: All posts in Wall UI are exposed.

Finally, all vulnerable content providers in Section 5 are not only accessible, but also faked information could be easily inserted into. For example in Figure 6, our attack demo could insert corresponding column name into a table called “message” in “OutboxMessageProvider”. Thus, attacker could insert carefully constructed content to phish user’s buddies.

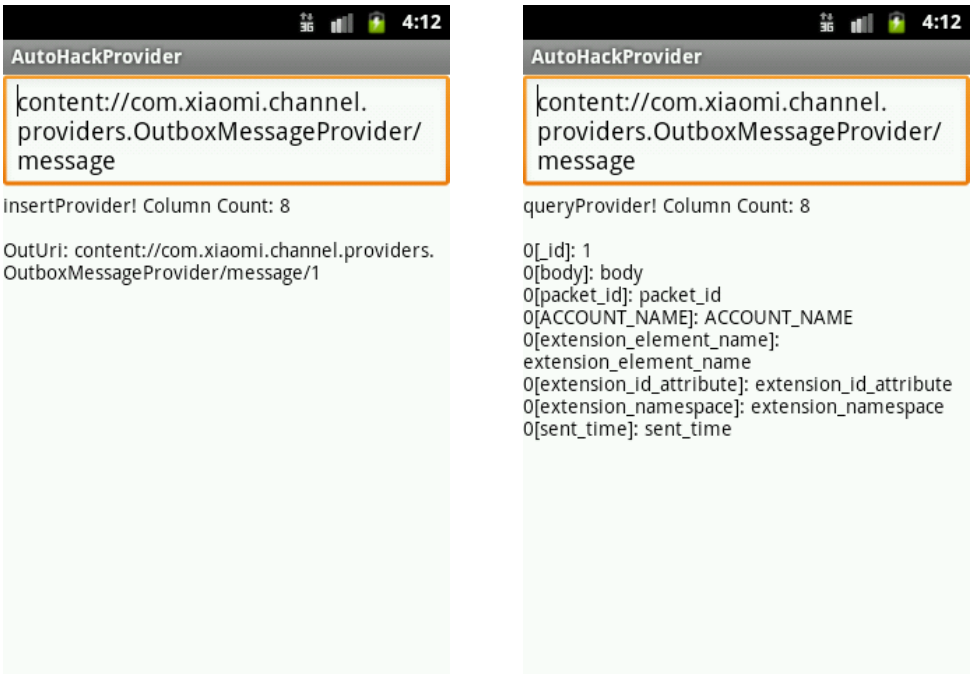

Figure 6: An attack demo about inserting faked content into a vulnerable table.

4 Solution

We are trying our best to contact *Xiaomi Inc.* 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

Among all 9 MiTalk's content providers, 5 of them are vulnerable and sensitive. These 5 content providers have 8 exploitable and sensitive tables in total, as shown in the following table:

Content Provider Authority	Table Name
com.xiaomi.channel.providers.BuddyProvider	buddy
com.xiaomi.channel.providers.OutboxMessageProvider	message
com.xiaomi.channel.providers.SmsContentProvider	sms
com.xiaomi.channel.providers.SmsContentProvider	attachments
com.xiaomi.channel.providers.SmsContentProvider	conversations
com.xiaomi.channel.providers.SystemMessageProvider	sysmsg
com.xiaomi.channel.providers.UploadedContactsContentProvider	contacts_info
com.xiaomi.channel.providers.WallProvider	posts