Vulnerability in GO Message Widget for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
Mar 2, 2012 at 5:59 PM HKT

Abstract

We found that GO Message Widget 1.9, 2.1 and 2.3 have a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including user's all attributes of sms (incoming and outgoing), user's contact numbers.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1407-vulnerability-in-GOMessageWidget.html

2 Description

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

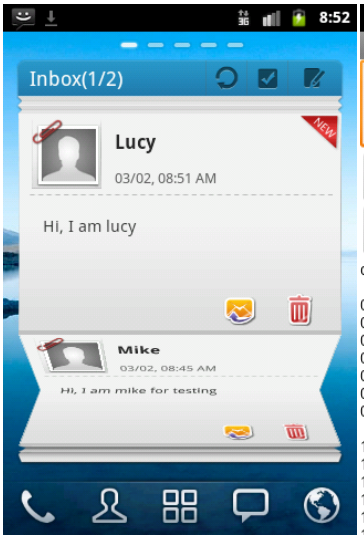
- `<provider android:name=".SmsProvider" android:multiprocess="false" android:authorities="com.gau.go.launcherex.gowidget.smswidget.provider2" android:grantUriPermissions="true" />`
- `<provider android:name=".DataProvider" android:multiprocess="false" android:authorities="com.gau.go.launcherex.gowidget.smswidget.provider" android:grantUriPermissions="true" />`

3 Impact

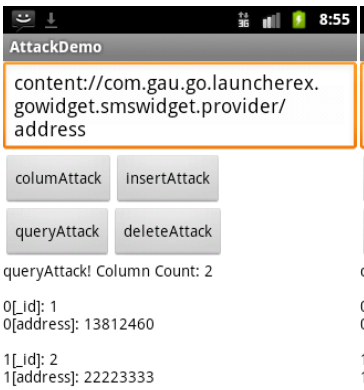
Please see the following snapshots generated by our arrack demo:

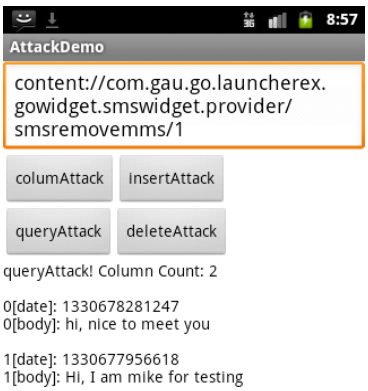
*** authors with equal contributions**


8:52
AttackDemo
content://com.gau.go.launcherex.gowidget.smswidget.provider/sms
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 7
0[_id]: 3
0[thread_id]: 2
0[address]: 22223333
0[person]: 2
0[date]: 1330678298404
0[read]: 0
0[body]: Hi, I am lucy
1[_id]: 1
1[thread_id]: 1
1[address]: 13812460
1[person]: null
1[date]: 1330677956618
1[read]: 1
1[body]: Hi, I am mike for testing

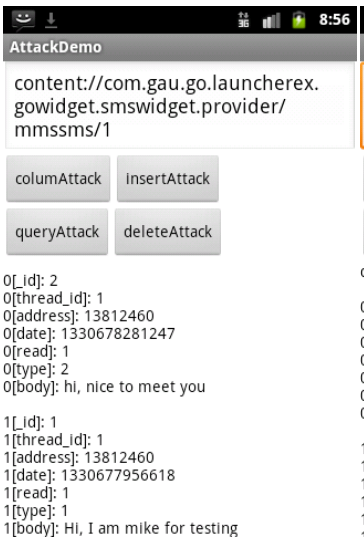

8:52
Inbox(1/2)
Lucy
03/02, 08:51 AM
Hi, I am lucy
Mike
03/02, 08:45 AM
Hi, I am mike for testing


8:54
AttackDemo
content://com.gau.go.launcherex.gowidget.smswidget.provider/conversations
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 7
0[_id]: 2
0[date]: 1330678298000
0[message_count]: 1
0[recipient_ids]: 2
0[snippet]: Hi, I am lucy
0[read]: 0
0[type]: 0
1[_id]: 1
1[date]: 1330678281000
1[message_count]: 2
1[recipient_ids]: 1
1[snippet]: hi, nice to meet you

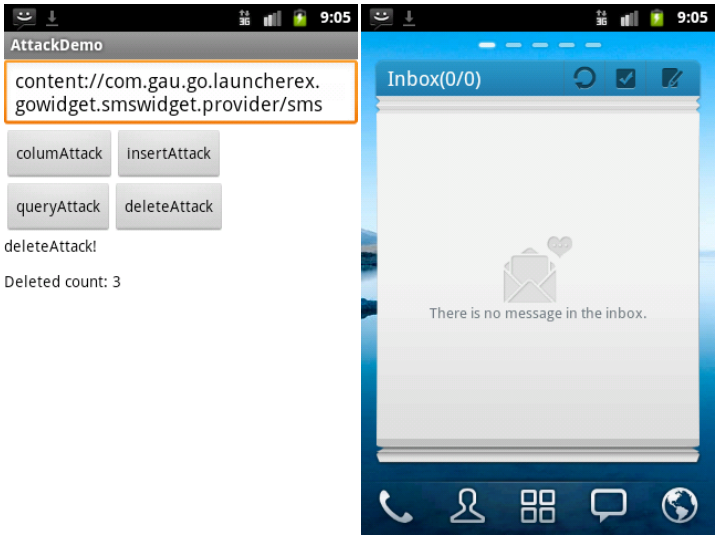

8:55
AttackDemo
content://com.gau.go.launcherex.gowidget.smswidget.provider/address
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 2
0[_id]: 1
0[address]: 13812460
1[_id]: 2
1[address]: 22223333


8:57
AttackDemo
content://com.gau.go.launcherex.gowidget.smswidget.provider/smsremovemms/1
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 2
0[date]: 1330678281247
0[body]: hi, nice to meet you
1[date]: 1330677956618
1[body]: Hi, I am mike for testing


8:55
AttackDemo
content://com.gau.go.launcherex.gowidget.smswidget.provider/smsbythread/1
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 7
0[_id]: 1
0[thread_id]: 1
0[address]: 13812460
0[person]: null
0[date]: 1330677956618
0[read]: 1
0[body]: Hi, I am mike for testing


8:56
AttackDemo
content://com.gau.go.launcherex.gowidget.smswidget.provider/mmssms/1
columAttack
insertAttack
queryAttack
deleteAttack
0[_id]: 2
0[thread_id]: 1
0[address]: 13812460
0[date]: 1330678281247
0[read]: 1
0[type]: 2
0[body]: hi, nice to meet you
1[_id]: 1
1[thread_id]: 1
1[address]: 13812460
1[date]: 1330677956618
1[read]: 1
1[type]: 1
1[body]: Hi, I am mike for testing


8:57
AttackDemo
content://com.gau.go.launcherex.gowidget.smswidget.provider/smssession
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 7
0[_id]: 3
0[thread_id]: 2
0[address]: 22223333
0[person]: 2
0[date]: 1330678298404
0[read]: 0
0[body]: Hi, I am lucy
1[_id]: 2
1[thread_id]: 1
1[address]: 13812460
1[person]: null
1[date]: 1330678281247



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.gau.go.launcherex.gowidget.smswidget.provider	sms
com.gau.go.launcherex.gowidget.smswidget.provider	contact
com.gau.go.launcherex.gowidget.smswidget.provider	photo
com.gau.go.launcherex.gowidget.smswidget.provider	smscount
com.gau.go.launcherex.gowidget.smswidget.provider	conversations
com.gau.go.launcherex.gowidget.smswidget.provider	address
com.gau.go.launcherex.gowidget.smswidget.provider	smsbythread
com.gau.go.launcherex.gowidget.smswidget.provider	mmssms
com.gau.go.launcherex.gowidget.smswidget.provider	smssession
com.gau.go.launcherex.gowidget.smswidget.provider	smsremovemms