Vulnerability in GO FBWidget 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 11:51 PM HKT

Abstract

We found that GO FBWidget 1.9 and 2.1 have a vulnerability that allows a crafted application to read and modify user's sensitive facebook information without permission, including user's facebook access token (in plaintext!), user's detailed information set in facebook (full name, about, email, birthday, website, gender, picture and etc.), detailed attributes of user's facebook status and comments,

1   Application Information

Please see the following link in our AppSec website:

http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1396-vulnerability-in-GOFBWidget.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.fbwidget.FacebookProvider"
  android:multiprocess="false"
  android:authorities="com.gau.go.launcherex.gowidget.fbwidget"
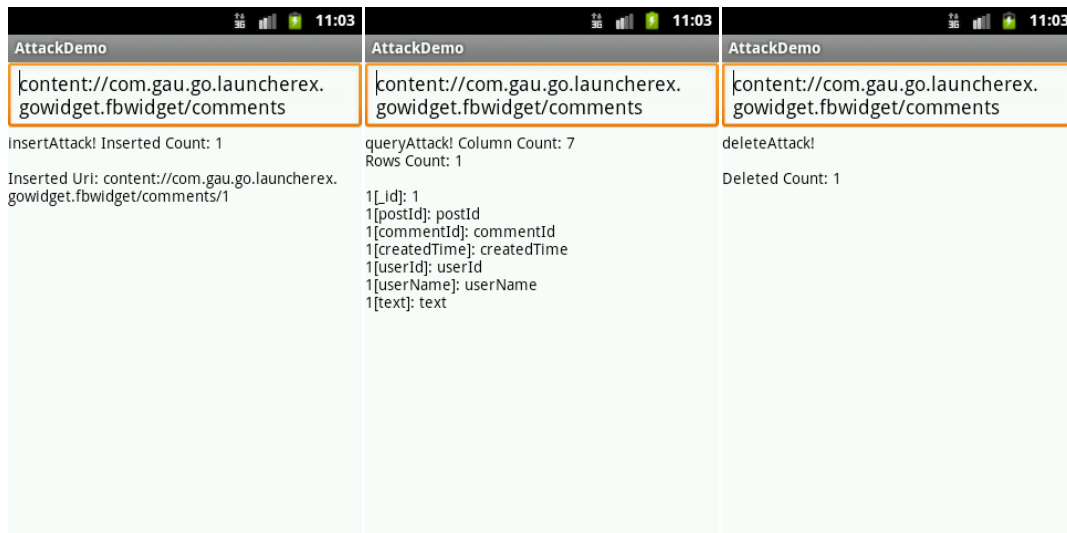 android:grantUriPermissions="true" />
  ```

## 3   Impact

Please see the following snapshots generated by our arrack demo:

**Settings - Insert**

🖧 ⓘⓘ 🔋 11:04

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/settings

insertAttack! Inserted Count: 1

Inserted Uri: content://com.gau.go.launcherex.
gowidget.fbwidget/settings/1

---

🖧 ⓘⓘ 🔋 11:04

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/settings

queryAttack! Column Count: 6
Rows Count: 1

1[_id]: 1
1[accesstoken]: accesstoken
1[updateindex]: updateindex
1[notification]: notification
1[keepalive]: keepalive
1[destop_exit]: destop_exit

---

🖧 ⓘⓘ 🔋 11:04

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/settings

deleteAttack!

Deleted Count: 1

---

🖧 ⓘⓘ 🔋 11:04

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/users

insertAttack! Inserted Count: 1

Inserted Uri: content://com.gau.go.launcherex.
gowidget.fbwidget/users/1

---

🖧 ⓘⓘ 🔋 11:04

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/users

queryAttack! Column Count: 14
Rows Count: 1

1[_id]: 1
1[userId]: userId
1[fullName]: fullName
1[firstName]: firstName
1[lastName]: lastName
1[link]: link
1[about]: about
1[birthday]: birthday
1[email]: email
1[website]: website
1[gender]: gender
1[timezone]: timezone
1[updatedTime]: updatedTime
1[picture]: picture

---

🖧 ⓘⓘ 🔋 11:04

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/users

deleteAttack!

Deleted Count: 1

---

🖧 ⓘⓘ 🔋 11:03

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/status

insertAttack! Inserted Count: 1

Inserted Uri: content://com.gau.go.launcherex.
gowidget.fbwidget/status/1

---

🖧 ⓘⓘ 🔋 11:03

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/status

queryAttack! Column Count: 20
Rows Count: 1

1[_id]: 1
1[postId]: postId
1[type]: type
1[createdTime]: createdTime
1[updatedTime]: updatedTime
1[inNews]: inNews
1[inWall]: inWall
1[fromName]: fromName
1[fromId]: fromId
1[toNames]: toNames
1[toIds]: toIds
1[text]: text
1[picture]: picture
1[link]: link
1[name]: name
1[caption]: caption
1[description]: description
1[source]: source
1[likes]: likes
1[comments]: comments

---

🖧 ⓘⓘ 🔋 11:03

AttackDemo

content://com.gau.go.launcherex.
gowidget.fbwidget/status

deleteAttack!

Deleted Count: 1

content://com.gau.go.launcherex. gowidget.fbwidget/comments

content://com.gau.go.launcherex. gowidget.fbwidget/comments

content://com.gau.go.launcherex. gowidget.fbwidget/comments

insertAttack! Inserted Count: 1

Inserted Uri: content://com.gau.go.launcherex. gowidget.fbwidget/comments/1

queryAttack! Column Count: 7
Rows Count: 1

1[_id]: 1
1[postId]: postId
1[commentId]: commentId
1[createdTime]: createdTime
1[userId]: userId
1[userName]: userName
1[text]: text

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.fbwidget | comments |
| com.gau.go.launcherex.gowidget.fbwidget | settings |
| com.gau.go.launcherex.gowidget.fbwidget | statistics |
| com.gau.go.launcherex.gowidget.fbwidget | status |
| com.gau.go.launcherex.gowidget.fbwidget | users |