Vulnerability in NetEase WeiboHD (网易微博 HD) for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
Feb 29, 2012 at 6:21 PM HKT

Abstract

We found that NetEase WeiboHD 1.0.0 Build 2012-01-05 18:00 has a vulnerability that allows a crafted application to read and modify user's sensitive weibo information without permission, including weibo accounts (username and password in plaintext!), all contents of user's weibo, user's location, user's configuration and etc.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1385-vulnerability-in-NetEaseWeiboHD.html

2 Description

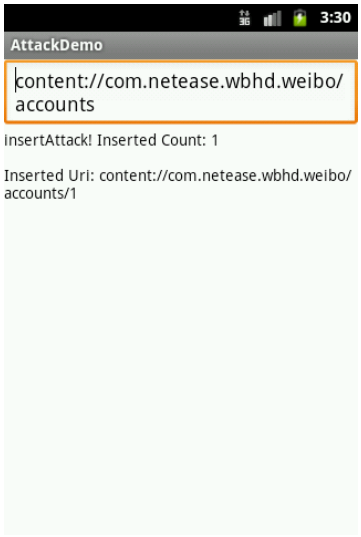
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

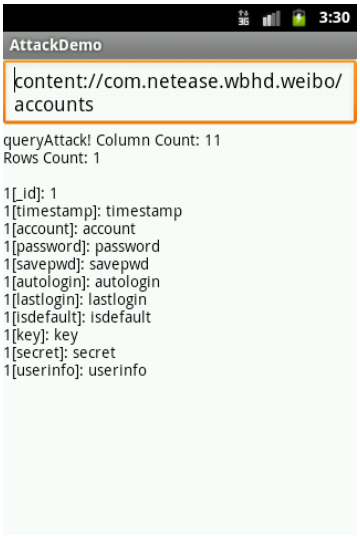
```
<provider android:name=".provider.weiboProvider"
android:multiprocess="true" android:authorities="com.netease.wbhd.weibo"
android:grantUriPermissions="true" />
<provider android:name="com.netease.frame.db.FrameProvider"
android:multiprocess="true"
android:authorities="com.netease.wbhd.framedb"
android:grantUriPermissions="true" />
```

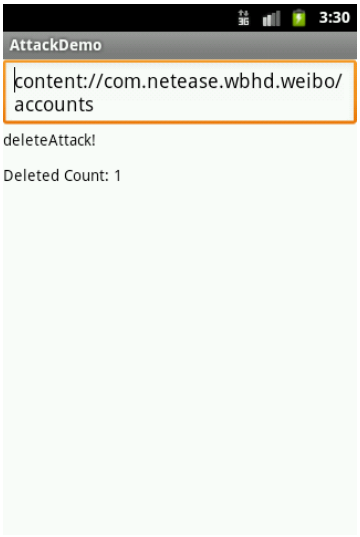
3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**

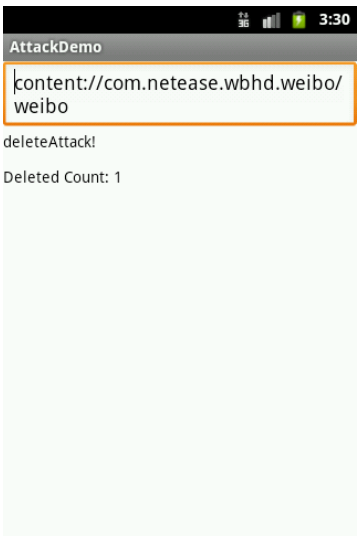

3:30
AttackDemo
content://com.netease.wbhd.weibo/accounts
insertAttack! Inserted Count: 1
Inserted Uri: content://com.netease.wbhd.weibo/accounts/1


3:30
AttackDemo
content://com.netease.wbhd.weibo/accounts
queryAttack! Column Count: 11
Rows Count: 1
1[_id]: 1
1[timestamp]: timestamp
1[account]: account
1[password]: password
1[savepwd]: savepwd
1[autologin]: autologin
1[lastlogin]: lastlogin
1[isdefault]: isdefault
1[key]: key
1[secret]: secret
1[userinfo]: userinfo

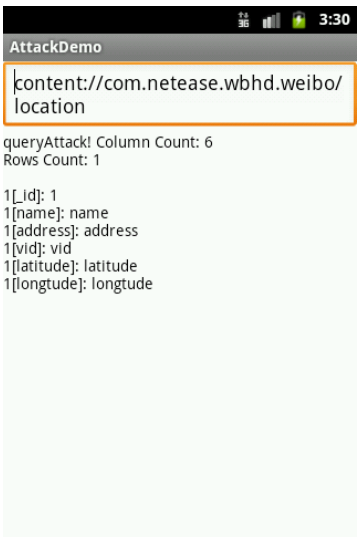

3:30
AttackDemo
content://com.netease.wbhd.weibo/accounts
deleteAttack!
Deleted Count: 1

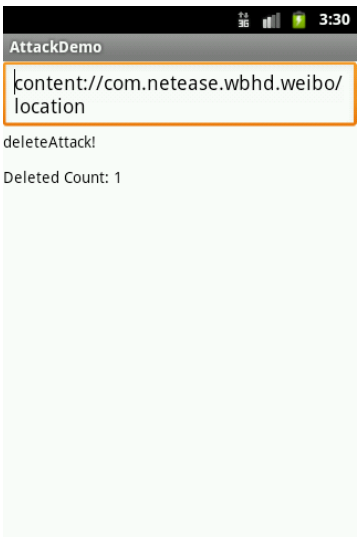

3:29
AttackDemo
content://com.netease.wbhd.weibo/weibo
insertAttack! Inserted Count: 1
Inserted Uri: content://com.netease.wbhd.weibo/weibo/1

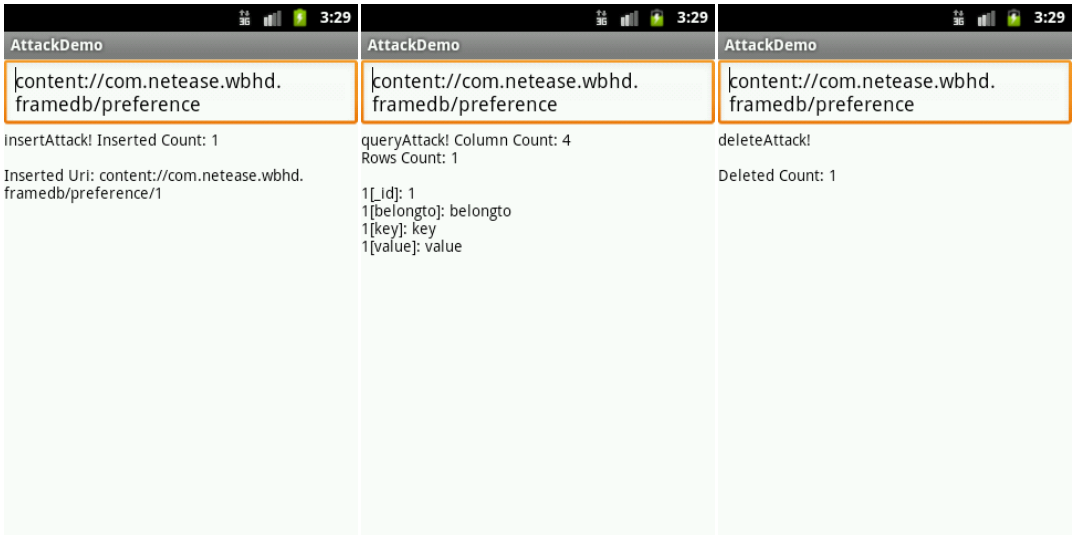

3:29
AttackDemo
content://com.netease.wbhd.weibo/weibo
queryAttack! Column Count: 11
Rows Count: 1
1[_id]: 1
1[belongto]: belongto
1[type]: type
1[tag]: tag
1[subtag]: subtag
1[weiboid]: weiboid
1[read]: read
1[timeline]: timeline
1[data1]: data1
1[data2]: data2
1[data3]: data3


3:30
AttackDemo
content://com.netease.wbhd.weibo/weibo
deleteAttack!
Deleted Count: 1


3:30
AttackDemo
content://com.netease.wbhd.weibo/location
insertAttack! Inserted Count: 1
Inserted Uri: content://com.netease.wbhd.weibo/location/1


3:30
AttackDemo
content://com.netease.wbhd.weibo/location
queryAttack! Column Count: 6
Rows Count: 1
1[_id]: 1
1[name]: name
1[address]: address
1[vid]: vid
1[latitude]: latitude
1[longtude]: longtude


3:30
AttackDemo
content://com.netease.wbhd.weibo/location
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.netease.wbhd.weibo	weibo
com.netease.wbhd.weibo	accounts
com.netease.wbhd.weibo	location
com.netease.wbhd.weibo	compress
com.netease.wbhd.weibo	photocapture
com.netease.wbhd.weibo	feedbacklog
com.netease.wbhd.framedb	preference
com.netease.wbhd.framedb	collector