Vulnerability in NetEaseWeibo (网易微博) 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 4:29 PM HKT

Abstract

We found that NetEaseWeibo 1.2.1 Build 2011-11-10 12:00 and 1.2.2 Build 2011-12-31 11:00 have 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 and etc.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1380-vulnerability-in-NetEaseWeibo.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="weibo"
android:grantUriPermissions="true" />
```

3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**


6:51
网易微博
t.163.com
帐号: happypeople12@163.com
密码: ••••••••••••••
登 录
注 册


7:04
AttackDemo
content://weibo/accounts
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 11
0[_id]: 1
0[timestamp]: 1330411877626
0[account]: hap[redacted]@163.com
0[password]: w[redacted]12
0[savepwd]: 1
0[autologin]: 1
0[lastlogin]: 1
0[isdefault]: 0
0[key]: null
0[secret]: null
0[userinfo]: {"in_groups":[],"sysTag":[],"status":
{"truncated":false},"location":"","followed_by":
false,"statuses_count":"0","url":"","id":
"3986649010551987080","following":false,
"blocking":false,"favourites_count":"0","email":
"happypeople12@163.com","verified":false,


7:05
AttackDemo
content://weibo/accounts
columAttack
insertAttack
queryAttack
deleteAttack
columAttack! Column Count: 11
0: _id
1: timestamp
2: account
3: password
4: savepwd
5: autologin
6: lastlogin
7: isdefault
8: key
9: secret
10: userinfo


7:04
我的资料
happypeople12
编辑资料
0 微博
16 关注
0 被关注
0 收藏
王晓渔
2158901被关注 358微博
取消关注
1978年底1979年初的西单民主墙、2003年的...
余秋雨
5156832被关注 39微博
取消关注
在整个民族的人格文化还没有重新建立的时候...
冯兴元
1137028被关注 1021微博
取消关注

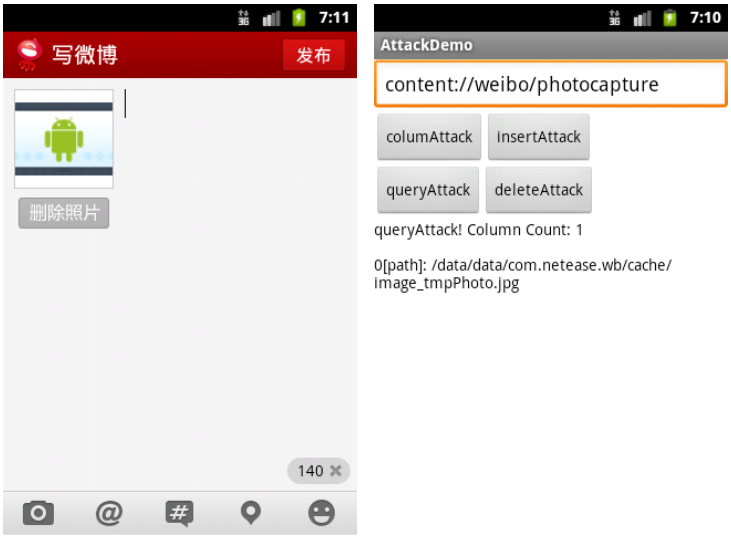

7:05
AttackDemo
content://weibo/weibo
columAttack
insertAttack
queryAttack
deleteAttack
"-5538698758505971617",
"root_in_reply_to_user_name":"夏小芽",
"retweet_user_name":"","in_reply_to_status_id":
"-2662398595893038851",
"root_in_reply_to_screen_name":"dybnu",
"created_at":"Tue Feb 28 14:49:39 +0800 2012",
"cursor_id":
"-5538698758505971617:1330411779685",
"root_comments_count":"0","favorited_at":"",
"retweet_user_id":"","is_retweet_by_user":false,
"comments_count":"1","text":"身份认证其实也可
以交给民间机构去做[鼓掌]","geo":{},
"in_reply_to_user_name":"夏小芽",
"root_in_reply_to_status_text":"美国人@睢鸠 你有
美国户口本了吗？上次我说了，Facebook野心很大
的，我很看好，Look！！现在看看～～ http:\/
\/126.fm\/4SUzjF","venue":{},
"root_in_reply_to_user_id":


7:05
AttackDemo
content://weibo/weibo
columAttack
insertAttack
queryAttack
deleteAttack
columAttack! Column Count: 7
0: _id
1: belongto
2: type
3: tag
4: weiboid
5: read
6: timeline


7:13
写微博
发布
@网易微博客户端 我在用android客户
端，版本号是1.2.2 Build 2011-12-31
11:00，手机型号sdk，SDK版本
号2.3.3。我遇到的问题是：rubbish
71


7:13
AttackDemo
content://weibo/feedbacklog
columAttack
insertAttack
queryAttack
deleteAttack
columAttack! Column Count: 2
0: _display_name
1: _size


7:13
AttackDemo
content://weibo/feedbacklog
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 2
0[_display_name]: ui_netease_weibo_log.zip
0[_size]: 63016



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
weibo	weibo
weibo	accounts
weibo	location
weibo	collector
weibo	compress
weibo	photocapture
weibo	feedbacklog