Vulnerability in Youdao Dictionary (有道字典) 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 5:48 PM HKT

Abstract

We found that Youdao Dictionary 1.6.1 and 2.0.1(2) have a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including Youdao Dictionary accounts (username and password in plaintext!), user's notes in using Youdao Dictionary, and etc.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1382-vulnerability-in-YoudaoDictionary.html

2 Description

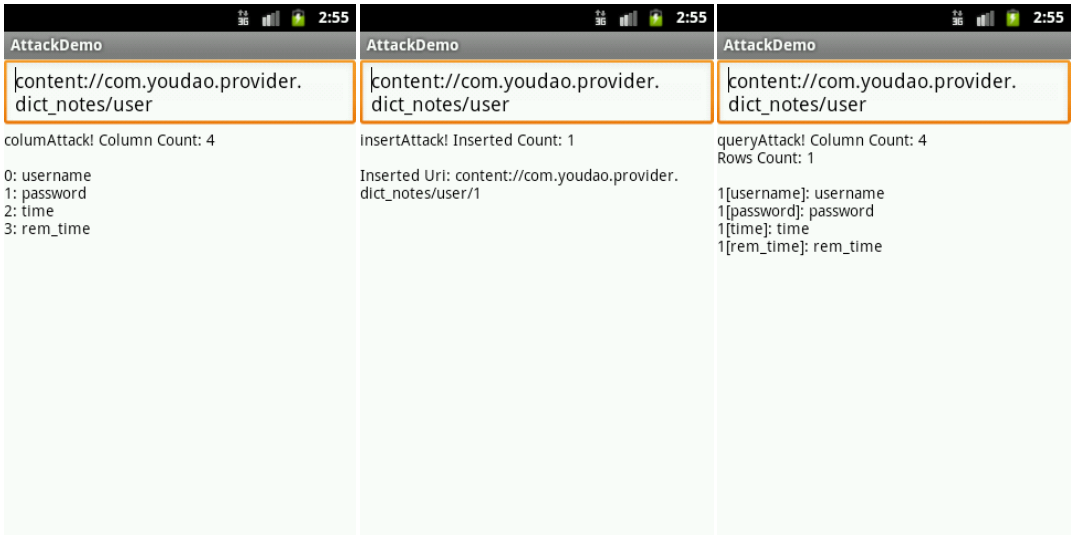
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

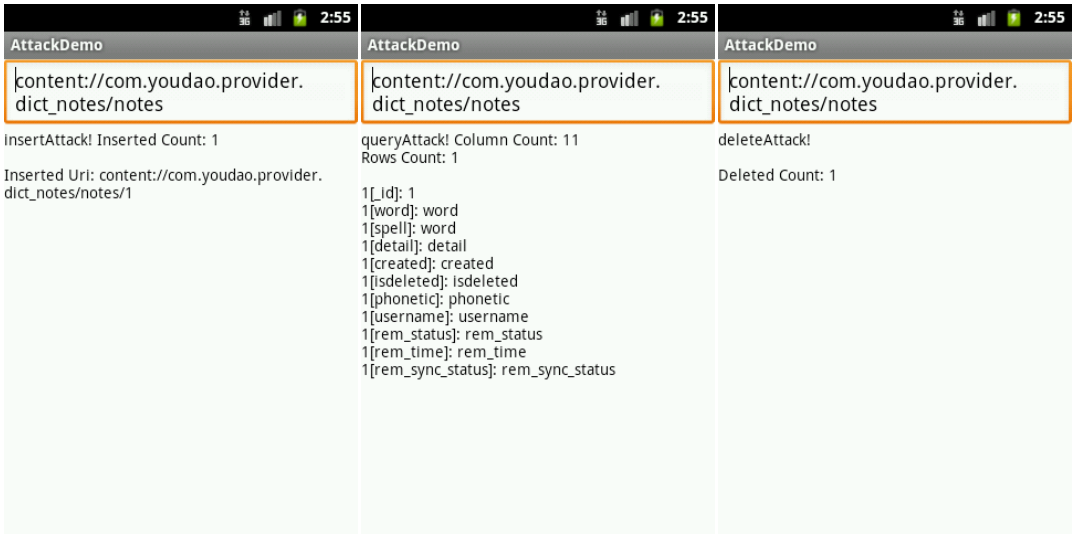
```
<provider android:name=".notes.DictNotesProvider"
android:authorities="com.youdao.provider.dict_notes" />
<provider android:name=".local.DictContentProvider"
android:authorities="com.youdao.provider.dict" />
<provider android:name=".review.NoteReviewInfoContentProvider"
android:authorities="com.youdao.provider.review" />
<provider android:name=".offlinedict.DictOfflineDictProvider"
android:authorities="com.youdao.provider.offlinedict" />
```

3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**





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.youdao.provider.dict_notes	notes
com.youdao.provider.dict_notes	user
com.youdao.provider.dict_notes	rawnotes

com.youdao.provider.dict_notes	note_tag_relations
com.youdao.provider.dict	words
com.youdao.provider.review	counts
com.youdao.provider.offlinedict	dicts