Vulnerability in 海豚浏览器 for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk

Mar 2, 2012 at 2:13 PM HKT

Abstract

We found that 海豚浏览器 6.3.1 and 7.2.1 have a vulnerability that allows a crafted application to read and modify user's sensitive browser information without permission, including user's bookmarks and downloads in 海豚浏览器.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1403-vulnerability-in-DolphinBrowserCN.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="mobi.mgeek.TunnyBrowser.BrowserProvider"
  android:multiprocess="true" android:authorities="tunny_browser_cn">
  ```

-
  ```
  <provider android:name="com.dolphin.browser.downloads.DownloadProvider"
  android:authorities="dolphin_browser_cn_downloads" />
  ```

-
  ```
  <provider android:name="mobi.mgeek.TunnyBrowser.BrowserProviderCN"
  android:authorities="dolphin_browser_cn" />
  ```

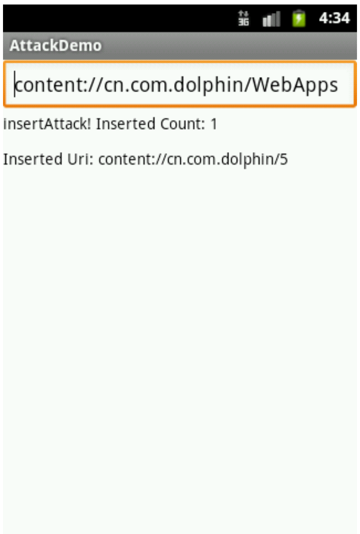
-
  ```
  <provider
  android:name="com.dolphin.browser.magazines.provider.WebzineProvider"
  android:authorities="dolphin_browser_cn_webzine" />
  ```

-
  ```
  <provider android:name="mgeek.provider.WebAppProvider"
  android:authorities="cn.com.dolphin" />
  ```

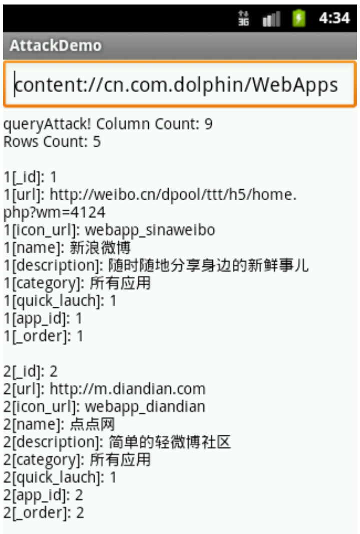
3 Impact

Please see the following snapshots generated by our arrack demo:

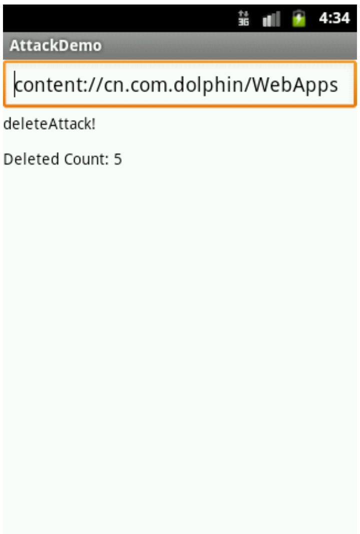
*** authors with equal contributions**



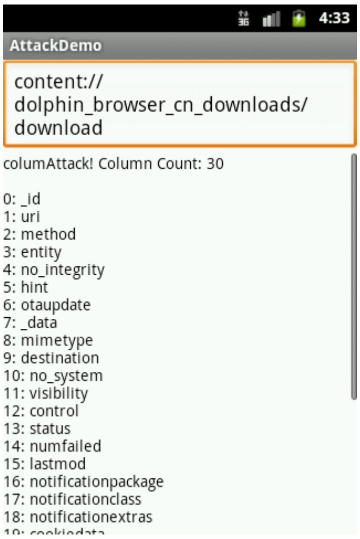
```
content://cn.com.dolphin/WebApps

insertAttack! Inserted Count: 1

Inserted Uri: content://cn.com.dolphin/5
```



```
content://cn.com.dolphin/WebApps

queryAttack! Column Count: 9
Rows Count: 5

1[_id]: 1
1[url]: http://weibo.cn/dpool/ttt/h5/home.
php?wm=4124
1[icon_url]: webapp_sinaweibo
1[name]: 新浪微博
1[description]: 随时随地分享身边的新鲜事儿
1[category]: 所有应用
1[quick_lauch]: 1
1[app_id]: 1
1[_order]: 1

2[_id]: 2
2[url]: http://m.diandian.com
2[icon_url]: webapp_diandian
2[name]: 点点网
2[description]: 简单的轻微博社区
2[category]: 所有应用
2[quick_lauch]: 1
2[app_id]: 2
2[_order]: 2
```



```
content://cn.com.dolphin/WebApps

deleteAttack!

Deleted Count: 5
```



```
content://
dolphin_browser_cn_downloads/
download

columAttack! Column Count: 30

0: _id
1: uri
2: method
3: entity
4: no_integrity
5: hint
6: otaupdate
7: _data
8: mimetype
9: destination
10: no_system
11: visibility
12: control
13: status
14: numfailed
15: lastmod
16: notificationpackage
17: notificationclass
18: notificationextras
19: cookiedata
```

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
dolphin_browser_cn_downloads	download
cn.com.dolphin	WebApps