Vulnerability in Dolphin Browser® HD for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
Mar 1, 2012 at 10:46 PM HKT

Abstract

We found that Dolphin Browser® HD 6.2.0, 7.2.1, 7.3.0 and 7.4.0 have a vulnerability that allows a crafted application to read and modify user's sensitive browser information without permission, including user's bookmarks, downloads, histories, most visited pages, and saved pages in Dolphin Browser® HD.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1392-vulnerability-in-DolphinBrowserHD.html

2 Description

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

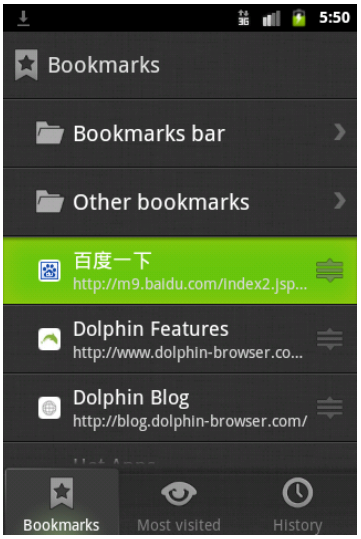
```
<provider android:name="mobi.mgeek.TunnyBrowser.BrowserProvider"
android:multiprocess="true" android:authorities="tunnybrowser">
<provider android:name="com.dolphin.browser.downloads.DownloadProvider"
android:authorities="tunnydownloads" />
<provider android:name="com.dolphin.browser.provider.BrowserProvider"
android:authorities="dolphinbrowserhd" />
<provider
android:name="com.dolphin.browser.voice.command.VoiceCommandProvider"
android:authorities="dolphin_voice_en" />
```

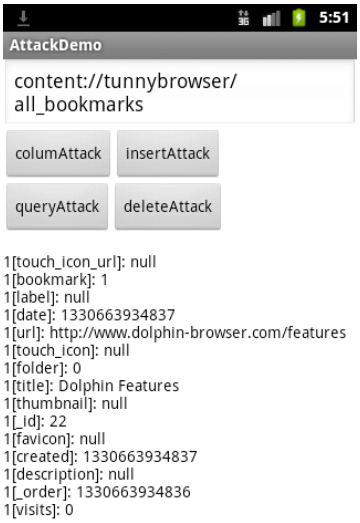
3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**

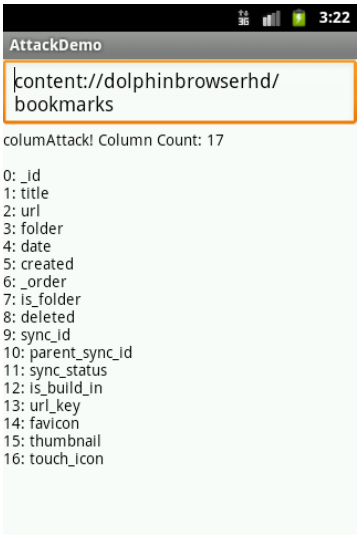

5:49
AttackDemo
content://tunnybrowser/bookmarks
columAttack
insertAttack
queryAttack
deleteAttack
28[title]: 百度一下
28[thumbnail]: null
28[_id]: 32
28[favicon]: null
28[created]: 1330667009074
28[description]: null
28[_order]: -1330667009074
28[visits]: 0
29[touch_icon_url]: null
29[bookmark]: 1
29[label]: null
29[date]: 1330667009113
29[url]: http://m9.baidu.com/index2.jsp?vit=fps&from=844b
29[touch_icon]: null
29[folder]: 0
29[title]: 百度一下

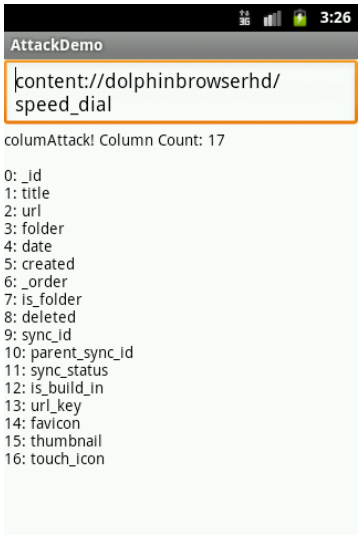

5:50
Bookmarks
Bookmarks bar
Other bookmarks
百度一下
http://m9.baidu.com/index2.jsp...
Dolphin Features
http://www.dolphin-browser.co...
Dolphin Blog
http://blog.dolphin-browser.com/
Bookmarks
Most visited
History

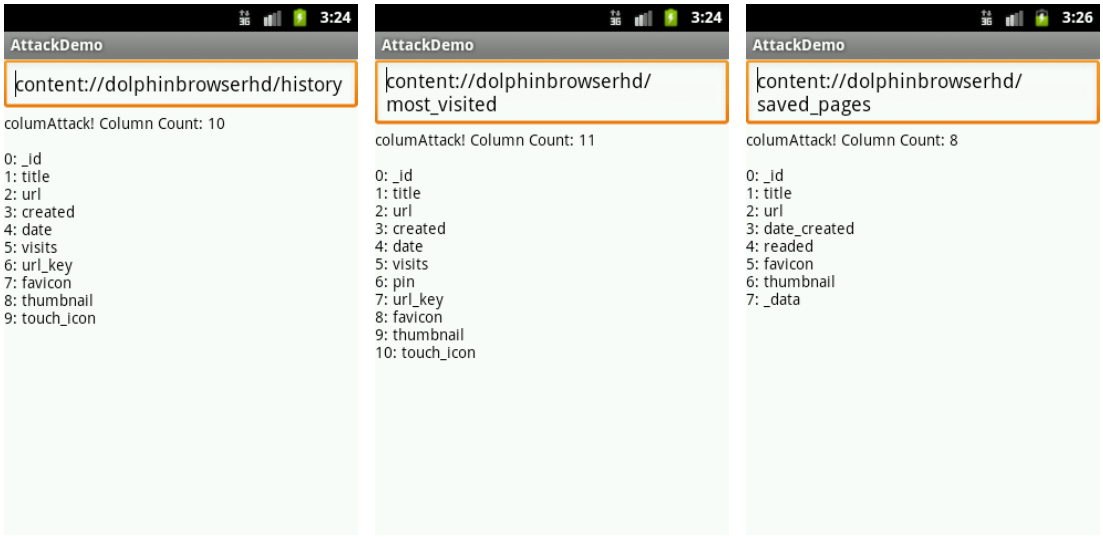

5:51
AttackDemo
content://tunnybrowser/all_bookmarks
columAttack
insertAttack
queryAttack
deleteAttack
1[touch_icon_url]: null
1[bookmark]: 1
1[label]: null
1[date]: 1330663934837
1[url]: http://www.dolphin-browser.com/features
1[touch_icon]: null
1[folder]: 0
1[title]: Dolphin Features
1[thumbnail]: null
1[_id]: 22
1[favicon]: null
1[created]: 1330663934837
1[description]: null
1[_order]: 1330663934836
1[visits]: 0


3:22
AttackDemo
content://tunnydownloads/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
20: useragent


5:58
AttackDemo
content://tunnydownloads/download
columAttack
insertAttack
queryAttack
deleteAttack
queryAttack! Column Count: 30
0[_id]: 1
0[uri]: http://img.yingyonghui.com/apk/6969/com.tsf.shell.1330660154900.apk
0[method]: 0
0[entity]: null
0[no_integrity]: null
0[hint]: com.tsf.shell.1330660154900.apk
0[otaupdate]: null
0[_data]: /mnt/sdcard/download/com.tsf.shell.1330660154900.apk
0[mimetype]: application/vnd.android.package-archive
0[destination]: null
0[no_system]: null
0[visibility]: 1


3:22
AttackDemo
content://dolphinbrowserhd/bookmarks
columAttack! Column Count: 17
0: _id
1: title
2: url
3: folder
4: date
5: created
6: _order
7: is_folder
8: deleted
9: sync_id
10: parent_sync_id
11: sync_status
12: is_build_in
13: url_key
14: favicon
15: thumbnail
16: touch_icon


3:26
AttackDemo
content://dolphinbrowserhd/speed_dial
columAttack! Column Count: 17
0: _id
1: title
2: url
3: folder
4: date
5: created
6: _order
7: is_folder
8: deleted
9: sync_id
10: parent_sync_id
11: sync_status
12: is_build_in
13: url_key
14: favicon
15: thumbnail
16: touch_icon



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
tunnybrowser	bookmarks
tunnybrowser	folders
tunnybrowser	all_bookmarks
tunnybrowser	reorder
tunnydownloads	download
dolphinbrowserhd	bookmarks
dolphinbrowserhd	bookmarks/folders
dolphinbrowserhd	history
dolphinbrowserhd	most_visited
dolphinbrowserhd	searches
dolphinbrowserhd	images
dolphinbrowserhd	speed_dial
dolphinbrowserhd	saved_pages
dolphin_voice_en	actions
dolphin_voice_en	build_in