

Vulnerability in NetFront Life Browser for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
Mar 14, 2012 at 3:52 PM HKT

Abstract

We found that NetFront Life Browser 2.2.0 and 2.3.0 have a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including user's bookmarks in NetFront Life Browser, user's history in NetFront Life Browser, user's downloads in NetFront Life Browser, and etc.

1 Application Information

Please see the following link in our AppSec website:

<http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1485-vulnerability-in-NetFrontLifeBrowser.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="com.access_company.android.nflifebrowser.app.nfbrowser.BookmarkProvider"
 android:authorities="com.access_company.android.nflifebrowser.bookmarkprovider.lite" />
```
- ```
<provider
  android:name="com.access_company.android.nflifebrowser.app.nfbrowser.ScrapProvider"
  android:authorities="com.access_company.android.nflifebrowser.scrapprovider.lite" />
```
- ```
<provider
 android:name="com.access_company.android.nflifebrowser.app.nfbrowser.DownloadProvider"
```

```
android:authorities="com.access_company.android.nflifebrowser.downloadpro
vider.lite" />
```

### 3 Impact

Please see the following snapshots generated by our arrack demo:

| AttackDemo                                                                                                                                        | AttackDemo                                                                                                                                                                                                                                           | AttackDemo                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| content://com.access_company.<br>android.nflifebrowser.<br>bookmarkprovider.lite/bookmarks                                                        | content://com.access_company.<br>android.nflifebrowser.<br>bookmarkprovider.lite/bookmarks                                                                                                                                                           | content://com.access_company.<br>android.nflifebrowser.<br>bookmarkprovider.lite/bookmarks |
| InsertAttack! Inserted Count: 1<br><br>Inserted Uri: content://com.access_company.<br>android.nflifebrowser.bookmarkprovider.lite/<br>bookmarks/1 | queryAttack! Column Count: 10<br>Rows Count: 1<br><br>1[_id]: 1<br>1[title]: title<br>1[url]: url<br>1[visits]: visits<br>1[date]: date<br>1[created]: created<br>1[type]: type<br>1[thumbnail]: thumbnail<br>1[favicon]: favicon<br>1[tagid]: tagid | deleteAttack!<br><br>Deleted Count: 1                                                      |

| AttackDemo                                                                                                                                      | AttackDemo                                                                                                                                                                                                                                           | AttackDemo                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| content://com.access_company.<br>android.nflifebrowser.<br>bookmarkprovider.lite/history                                                        | content://com.access_company.<br>android.nflifebrowser.<br>bookmarkprovider.lite/history                                                                                                                                                             | content://com.access_company.<br>android.nflifebrowser.<br>bookmarkprovider.lite/history |
| InsertAttack! Inserted Count: 1<br><br>Inserted Uri: content://com.access_company.<br>android.nflifebrowser.bookmarkprovider.lite/<br>history/1 | queryAttack! Column Count: 10<br>Rows Count: 1<br><br>1[_id]: 1<br>1[title]: title<br>1[url]: url<br>1[visits]: visits<br>1[date]: date<br>1[created]: created<br>1[type]: type<br>1[thumbnail]: thumbnail<br>1[favicon]: favicon<br>1[tagid]: tagid | deleteAttack!<br><br>Deleted Count: 1                                                    |

|                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>downloadprovider.lite/downloads</p> <p>InsertAttack! Inserted Count: 1</p> <p>Inserted Uri: content://com.access_company.<br/>android.nflifebrowser.downloadprovider.lite/<br/>downloads/1</p> | <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>downloadprovider.lite/downloads</p> <p>queryAttack! Column Count: 8<br/>Rows Count: 1</p> <p>1[_id]: 1<br/>1[filename]: filename<br/>1[filesize]: filesize<br/>1[mimetype]: mimetype<br/>1[state]: state<br/>1[url]: url<br/>1[contentlength]: contentlength<br/>1[etag]: etag</p> | <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>downloadprovider.lite/downloads</p> <p>deleteAttack!</p> <p>Deleted Count: 1</p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>scrapprovider.lite/scrapbooks</p> <p>InsertAttack! Inserted Count: 1</p> <p>Inserted Uri: content://com.access_company.<br/>android.nflifebrowser.scrapprovider.lite/<br/>scrapbooks/1</p> | <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>scrapprovider.lite/scrapbooks</p> <p>queryAttack! Column Count: 6<br/>Rows Count: 1</p> <p>1[_id]: 1<br/>1[title]: title<br/>1[thumbnail]: thumbnail<br/>1[created]: created<br/>1[updated]: updated<br/>1[share]: share</p> | <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>scrapprovider.lite/scrapbooks</p> <p>deleteAttack!</p> <p>Deleted Count: 1</p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>scrapprovider.lite/scraps</p> <p>InsertAttack! Inserted Count: 1</p> <p>Inserted Uri: content://com.access_company.<br/>android.nflifebrowser.scrapprovider.lite/scraps/1</p> | <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>scrapprovider.lite/scraps</p> <p>queryAttack! Column Count: 11<br/>Rows Count: 1</p> <p>1[_id]: 1<br/>1[image]: image<br/>1[page_title]: page_title<br/>1[page_url]: page_url<br/>1[created]: created<br/>1[scrapbook]: scrapbook<br/>1[x]: x<br/>1[y]: y<br/>1[width]: width<br/>1[height]: height<br/>1[z_index]: z_index</p> | <p>AttackDemo</p> <p>content://com.access_company.<br/>android.nflifebrowser.<br/>scrapprovider.lite/scraps</p> <p>deleteAttack!</p> <p>Deleted Count: 1</p> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 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.