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

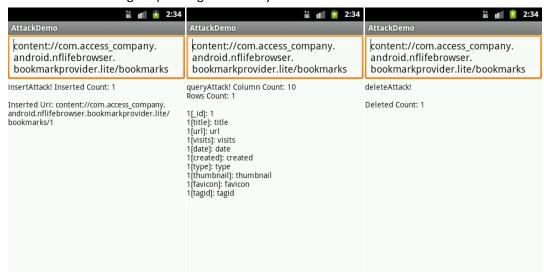
2 Description

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

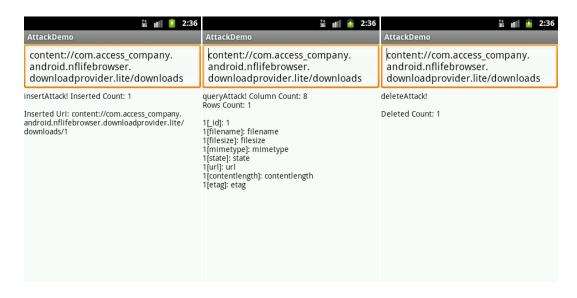
loadProvider"

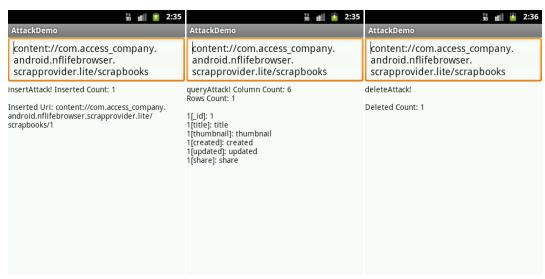
3 Impact

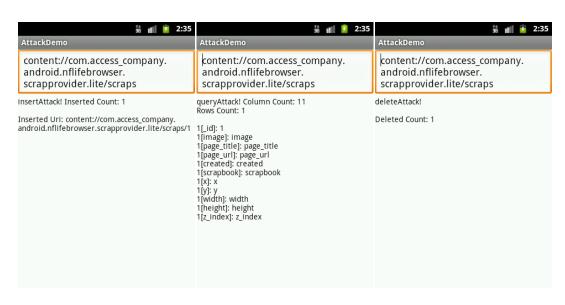
Please see the following snapshots generated by our arrack demo:











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.