Vulnerability in UCMobile BloveStorm (来电通) for Android

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

Mar 13, 2012 at 10:14 PM HKT

Abstract

We found that UCMobile BloveStorm 2.2.0 and 3.2.1 have a vulnerability that allows a crafted application to read and modify user’s sensitive information without permission, including private call log (phone number and time), private sms log (phone number, time and sms content), intercepted call log in BloveStorm, and intercepted sms log in BloveStorm.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1478-vulnerability-in-UCMobileBloveStorm.html

2 Description

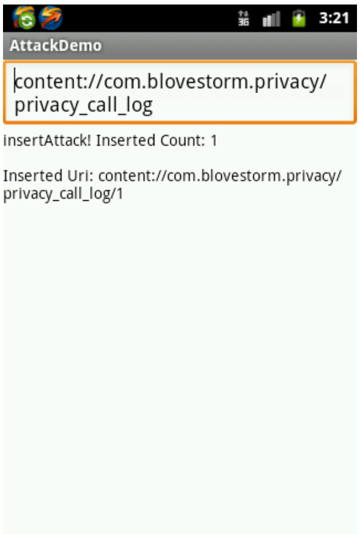
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

```
●  <provider android:name=".common.InterceptProvider"
   android:authorities="com.blovestorm.intercept" />
●  <provider android:name=".common.PrivacyProvider"
   android:authorities="com.blovestorm.privacy" />
●  <provider android:name=".common.CallRingProvider"
   android:authorities="com.blovestorm.callringlog" />
```

3 Impact

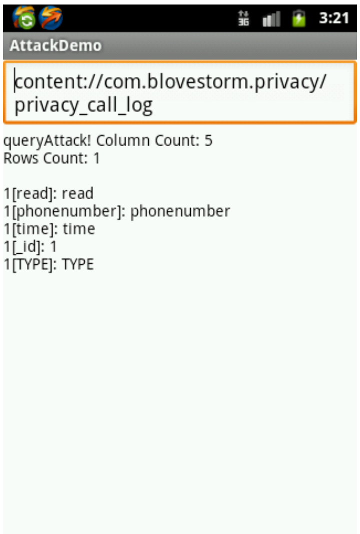
Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**



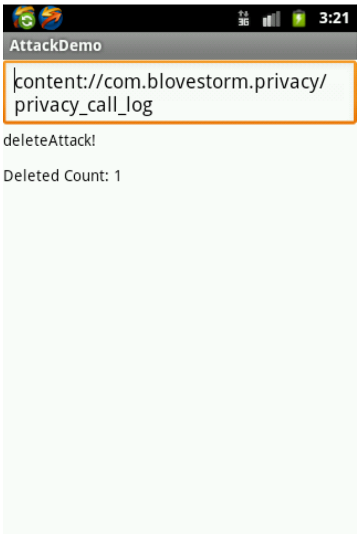
content://com.blovestorm.privacy/privacy_call_log

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.blovestorm.privacy/
privacy_call_log/1
```



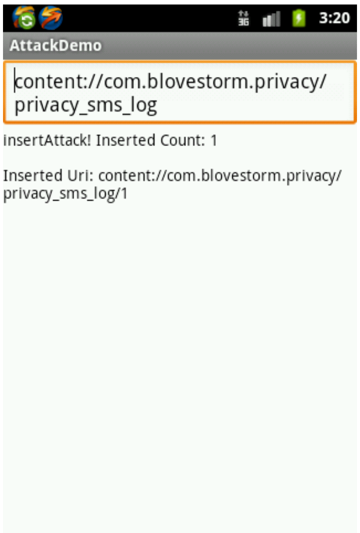
content://com.blovestorm.privacy/privacy_call_log

```
queryAttack! Column Count: 5
Rows Count: 1

1[read]: read
1[phonenumber]: phonenumber
1[time]: time
1[_id]: 1
1[TYPE]: TYPE
```



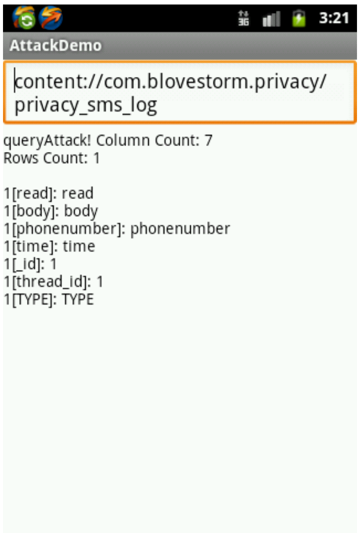
content://com.blovestorm.privacy/privacy_call_log

```
deleteAttack!

Deleted Count: 1
```



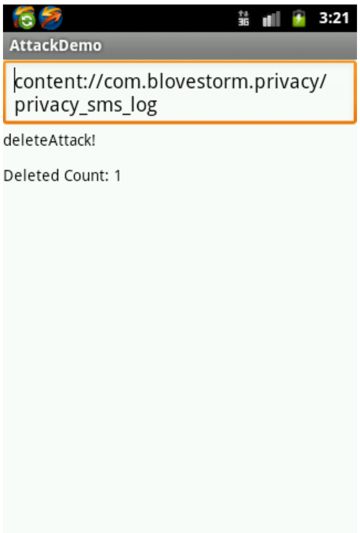
content://com.blovestorm.privacy/privacy_sms_log

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.blovestorm.privacy/
privacy_sms_log/1
```



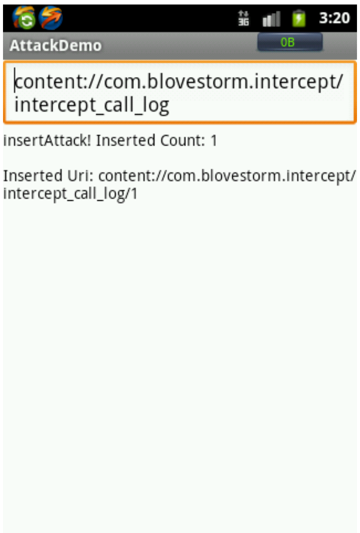
content://com.blovestorm.privacy/privacy_sms_log

```
queryAttack! Column Count: 7
Rows Count: 1

1[read]: read
1[body]: body
1[phonenumber]: phonenumber
1[time]: time
1[_id]: 1
1[thread_id]: 1
1[TYPE]: TYPE
```



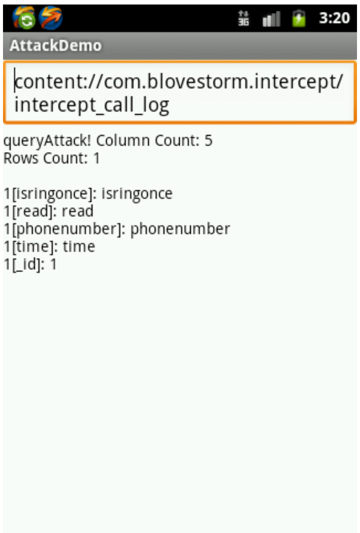
content://com.blovestorm.privacy/privacy_sms_log

```
deleteAttack!

Deleted Count: 1
```



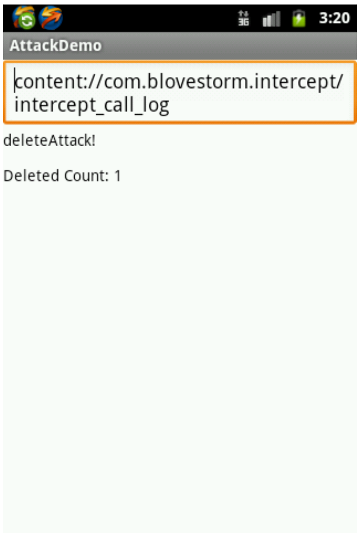
content://com.blovestorm.intercept/intercept_call_log

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.blovestorm.intercept/
intercept_call_log/1
```



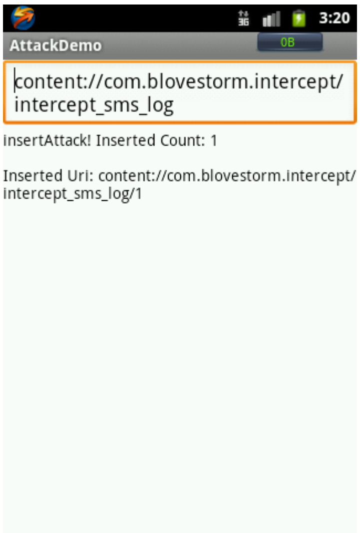
content://com.blovestorm.intercept/intercept_call_log

```
queryAttack! Column Count: 5
Rows Count: 1

1[isringonce]: isringonce
1[read]: read
1[phonenumber]: phonenumber
1[time]: time
1[_id]: 1
```



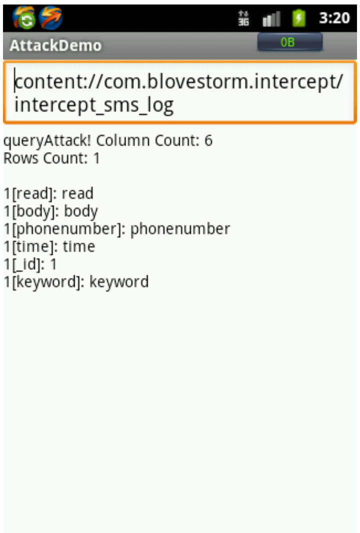
content://com.blovestorm.intercept/intercept_call_log

```
deleteAttack!

Deleted Count: 1
```



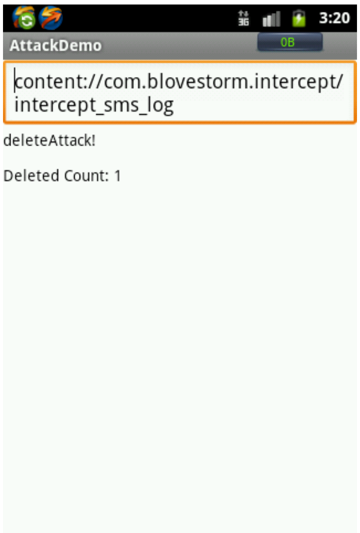
content://com.blovestorm.intercept/intercept_sms_log

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.blovestorm.intercept/
intercept_sms_log/1
```



content://com.blovestorm.intercept/intercept_sms_log

```
queryAttack! Column Count: 6
Rows Count: 1

1[read]: read
1[body]: body
1[phonenumber]: phonenumber
1[time]: time
1[_id]: 1
1[keyword]: keyword
```



content://com.blovestorm.intercept/intercept_sms_log

```
deleteAttack!

Deleted Count: 1
```

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.