

Subject: **Advisory Prevention Against Cyber Espionage (Advisory No 21)**
Apr 18

1. **Introduction.** A new vulnerability has been disclosed in iOS Camera App that could be exploited to redirect users to a malicious website without their knowledge. The vulnerability affects Apple's latest iOS 11 mobile operating system for iPhone/iPad/iPod touch devices and resides in the built-in QR code reader.

2. **Technical Analysis**

- a. With iOS 11, Apple introduced a new feature that gives users ability to automatically read QR codes using their iPhone's native camera app without requiring any third-party QR code reader app.
- b. You need to open the Camera app on your iPhone or iPad and point the device at a QR code. If the code contains any URL, it will give you a notification with the link address, asking you to tap to visit it in Safari browser.
- c. The URL parser of built-in QR code reader for iOS camera app fails to detect the hostname in the URL, which allows attackers to manipulate the displayed URL in the notification, tricking users to visit malicious websites instead.

3. **Affected Products.** This vulnerability affects all versions of iPhone, iPad and iPod till update.

4. **Recommendations**

- a. Keep iOS firmware up to date.
- b. Don't jailbreak your iPhone and only install applications with good reputation from Apple app store
- c. Don't download attachments from emails unless you are sure about the source.