
***Issued 4/24/18***

**Apple Device Users, Stay Away from QR Codes until you Upgrade**

Apple has plugged four vulnerabilities, two of which could be exploited to execute arbitrary code if a user visits a malicious website. The two critical vulnerabilities (CVE-2018-4200, CVE-2018-4204) affect WebKit, the web browser engine used in Apple's Safari browser (both the Mac and the iOS version). They have been discovered and flagged by Ivan Fratric of Google Project Zero and Richard Zhu working with Trend Micro's Zero Day Initiative. The other two vulnerabilities are less severe, but still can be exploited to do some damage. CVE-2018-4187, flagged both by Zhiyang Zeng of Tencent Security Platform Department and IT security consultant Roman Mueller, is a QR code URL parser bug that could be exploited by attackers to direct users to malicious sites: Mueller found that it's easy to construct a QR code which will show an innocent-looking hostname in the notification shown by the device while the link is pointing to a malicious site. More information on how this bug can be exploited can be found here. Apple hasn't released updates for tvOS, watchOS or iTunes, but judging by previous experience we can expect them to be released soon as WebKit is included in those offerings and WebKit patches are usually implemented in those updates.