computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2017-008

Broadcom Critical Wi-Fi SoC Vulnerability in iOS and Android

April 7, 2017 — v1.0

History:

- *07/04/2017 — v1.0: Initial publication*

Summary

The vulnerability resides in a widely used Wi-Fi chipset manufactured by Broadcom and used in both iOS and Android devices. An attacker within range may be able to execute arbitrary code on the Wi-Fi chip. Google Project Zero researcher Gal Beniamini, who discovered the flaw said it allowed the execution of malicious code by Wi-Fi proximity alone, requiring no user interaction [1].

Technical Details

The proof-of-concept exploit [1] developed by Gal Beniamini uses Wi-Fi frames that contain irregular values. The values cause the firmware running on Broadcom's wireless system-on-chip (SoC) to overflow its stack. By using the frames to target timers responsible for carrying out regularly occurring events such as performing scans for adjacent networks, specific regions of device memory are overwritten with arbitrary *shellcode*. Proof-of-concept code does nothing more than write a benign value to a specific memory address. Attackers could exploit the same series of flaws to execute malicious code on vulnerable devices within range of a rogue access point [2].

Products Affected

Mobile devices equipped with Broadcom WiFi SoC including (but not limited to) [5]:

- iPhone 5 through to iPhone 7,
- Android Google Nexus,
- Samsung Galaxy latest flagships.

Besides smartphones and tablets, many other devices with Broadcom Wi-Fi chips could also be affected, including Wi-Fi routers, according to Beniamini [5,1]. However, no such devices have been identified at this time.

Recommendations

Apple patched the vulnerability with release of iOS 10.3.1. Google is in the process of releasing an update in its April security bulletin for its Nexus devices. The fix is available only to a select number of device models, and even then it can take two weeks or more to be available as an over-the-air update to those who are eligible [2].

At the moment, it is not clear if there are effective workarounds available for vulnerable devices. Turning off Wi-Fi is one possibility, but as revealed in recent research into an unrelated Wi-Fi-related weakness involving Android phones, devices often relay on Wi-Fi frames even when Wi-Fi is turned off, for example when hen Wi-Fi-based location settings are enabled [3,4].

References

[1] https://googleprojectzero.blogspot.be/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html

[2] https://arstechnica.com/security/2017/04/wide-range-of-android-phones-vulnerable-to-device-hijacks-over-wi-fi/?comments=1

[3] https://arxiv.org/pdf/1703.02874v1.pdf

[4] https://arstechnica.com/security/2017/03/shielding-mac-addresses-from-stalkers-is-hard-android-is-failing-miserably/

[5] http://www.zdnet.com/article/iphone-android-hit-by-broadcom-wi-fi-chip-bugs-now-apple-google-plug-flaws/