

Subject:- Prevention Against Apple iPhone WiFi Chip Exploit (Advisory No 16) October, 2017

1. **Introduction.** A security vulnerability named CVE-2017-11120 has been discovered by a researcher at Google Security. It resides in Apple's iPhone and other devices with Broadcom Wi-Fi chips running firmware version BCM4355C0.
2. **Other Affected Devices**
 - a. Android smart phones
 - b. Smart TVs
 - c. Apple TV
3. **Mode, of Operation.** The flaw once exploited will allow an attacker to insert a backdoor into Broadcom chip's firmware, allowing remote read/ write commands to be issued to the firmware via crafted action frames, thus allowing easy remote control over the Wi-Fi chip.
4. **Recommendations.** In order to prevent remote access over the VViFi chip, the following is suggested:-
 - a. Update iPhones to iOS 11
 - b. Update AppleTVs to tvOS 11
 - c. Update Android devices to 2017-09-05 security patch level