
***Issued 4/6/17***

## Millions Of Smartphones Using Broadcom Wi-Fi Chip Can Be Hacked Over-the-Air

Millions of smartphones and smart gadgets, including Apple iOS and many Android handsets from various manufacturers, equipped with Broadcom Wifi chips are vulnerable to over-the-air hijacking without any user interaction.

Just yesterday, Apple rushed out an emergency iOS 10.3.1 patch update to address a serious bug that could allow an attacker within same Wifi network to remotely execute malicious code on the Broadcom WiFi SoC (Software-on-Chip) used in iPhones, iPads, and iPods.

The vulnerability was described as the stack buffer overflow issue and was discovered by Google's Project Zero staffer Gal Beniamini, who today detailed his research on a lengthy blog post, saying the flaw affects not only Apple but all those devices using Broadcom's Wi-Fi stack.

Attackers with high skills can also deploy malicious code to take full control over the victim's device and install malicious apps, like banking Trojans, ransomware, and adware, without the victim's knowledge. So, to exploit the flaw, an attacker needs to be within the WiFi range of the affected device to silently take over it.

"While the firmware implementation on the Wi-Fi SoC is incredibly complex, it still lags behind in terms of security," Beniamini explains. "Specifically, it lacks all basic exploit mitigations – including stack cookies, safe unlinking and access permission protection."

The researcher also detailed a proof-of-concept Wi-Fi remote code execution exploit in the blog post and successfully performed it on a then-fully updated (now fixed) Nexus 6P, running Android 7.1.1 version NUF26K – the latest available Nexus device at the time of testing in February.

Google Project Zero team reported the issue to Broadcom in December. Since the flaw is in Broadcom's code, smartphone makers had to wait for a patch from the chip vendor before testing the patch and pushing it out to their own user base.

Both Apple and Google addressed the vulnerability with security updates released on Monday, with Google delivering updates via its Android April 2017 Security Bulletin and Apple releasing the iOS 10.3.1 update.