iPhone zero-click Wi-Fi exploit is one of the most breathtaking hacks ever

Dan Goodin - 12/2/2020, 1:34 PM

WI-FI PACKETS OF DEATH —

Before Apple patch, Wi-Fi packets could steal photos. No interaction needed. Over the air.

Enlarge / That's a lot of screen.

Samuel Axon

Earlier this year, Apple patched one of the most breathtaking iPhone vulnerabilities ever: a memory corruption bug in the iOS kernel that gave attackers remote access to the entire device—over Wi-Fi, with no user interaction required at all. Oh, and exploits were wormable—meaning radio-proximity exploits could spread from one nearby device to another, once again, with no user interaction needed.

This Wi-Fi packet of death exploit was devised by Ian Beer, a researcher at Project Zero, Google's vulnerability research arm. In a 30,000-word post published on Tuesday afternoon, Beer described the vulnerability and the proof-of-concept exploit he spent six months developing single-handedly. Almost immediately, fellow security researchers took notice.

Beware of dodgy Wi-Fi packets

"This is a fantastic piece of work," Chris Evans, a semi-retired security researcher and executive and the founder of Project Zero, said in an interview. "It really is pretty serious. The fact you don't have to really interact with your phone for this to be set off on you is really quite scary. This attack is just you're walking along, the phone is in your pocket, and over Wi-Fi someone just worms in with some dodgy Wi-Fi packets."

Beer's attack worked by exploiting a buffer overflow bug in a driver for AWDL, an Apple-proprietary mesh networking protocol that makes things like Airdrop work. Because drivers reside in the kernel—one of the most privileged parts of any operating system—the AWDL flaw had the potential for serious hacks. And because AWDL parses Wi-Fi packets, exploits can be transmitted over the air, with no indication that anything is amiss.

"Imagine the sense of power an attacker with such a capability must feel," Beer wrote. "As we all pour more and more of our souls into these devices, an attacker can gain a treasure trove of information on an unsuspecting target."

Beer developed several different exploits. The most advanced one installs an implant that has full access to the user's personal data, including emails, photos, messages, and passwords and crypto keys stored in the keychain. The attack uses a laptop, a Raspberry Pi, and some off-the-shelf Wi-Fi adapters. It takes about two minutes to install the prototype implant, but Beer said that with more work a better written exploit could deliver it in a "handful of seconds." Exploits work only on devices that are within Wi-Fi range of the attacker.

Below is a video of the exploit in action. The victim's iPhone 11 Pro is in a room that's separated from the attacker by a closed door.

AWDL Implant Demo.

Beer said that Apple fixed the vulnerability before the launch of the COVID-19 contact-tracing interfaces put into iOS 13.5 in May. The researcher said he has no evidence the vulnerability was ever exploited in the wild, although he noted that at least one exploit seller was aware of the critical bug in May, seven months before today's disclosure. Apple figures show that the vast majority of iPhones and iPads are updated regularly.

The beauty and impressiveness of the hack is that it relies on a single bug to wirelessly access secrets locked away in what's arguably the world's most hardened and secure consumer device. If a single person could do all of this in six months, just think what a better-resourced hacking team is capable of.