Issued 9/12/17

New Bluetooth Vulnerability can Hack a Phone in 10 Seconds

Security company Armis has found a collection of eight exploits, collectively called BlueBorne, that can allow an attacker access to your phone without touching it. The attack can allow access to computers and phones, as well as IoT devices. "Armis believes many more vulnerabilities await discovery in the various platforms using Bluetooth. These vulnerabilities are fully operational, and can be successfully exploited, as demonstrated in our research. The BlueBorne attack vector can be used to conduct a large range of offenses, including remote code execution as well as Man-in-The-Middle attacks. "BlueBorne affects pretty much every device we use said Ralph Echemendia, CEO of Seguru. The vector allows the hacker to identify a device, connect to it via Bluetooth, and then begin controlling the screen and apps. It's not completely secretive, however, because in activating the exploits you "wake up" the device. The complex vector begins by finding a device to hack. This includes forcing the device to give up information about itself and then, ultimately, release keys and passwords "in an attack that very much resembles heartbleed," the exploit that forced many web servers to display passwords and other keys remotely. The next step is a set of code executions that allows for full control of the device. "This vulnerability resides in the Bluetooth Network Encapsulation Protocol (BNEP) service, which enables internet sharing over a Bluetooth connection (tethering). Due to a flaw in the BNEP service, a hacker can trigger a surgical memory corruption, which is easy to exploit

and enables him to run code on the device, effectively granting him complete control," write the researchers. Finally, when the hacker has access they are able to begin streaming data from the device in a "man-in-the-middle" attack. "The vulnerability resides in the PAN profile of the Bluetooth stack, and enables the attacker to create a malicious network interface on the victim's device, re-configure IP routing and force the device to transmit all communication through the malicious network interface. This attack does not require any user interaction, authentication or pairing, making it practically invisible." Windows and iOS phones are protected and Google users are receiving a patch today. Other devices running older versions of Android and Linux could be vulnerable. How do you stay safe? Keep all of your devices updated regularly and be wary of older IoT devices. In most cases the problems associated with BlueBorne vectors should be patched by major players in the electronics space but less popular devices could still be vulnerable to attack. "New solutions are needed to address the new airborne attack vector, especially those that make air gapping irrelevant. Additionally, there will need to be more attention and research as new protocols are using for consumers and businesses alike. With the large number of desktop, mobile, and IoT devices only increasing, it is critical we can ensure these types of vulnerabilities are not exploited," wrote Armis.