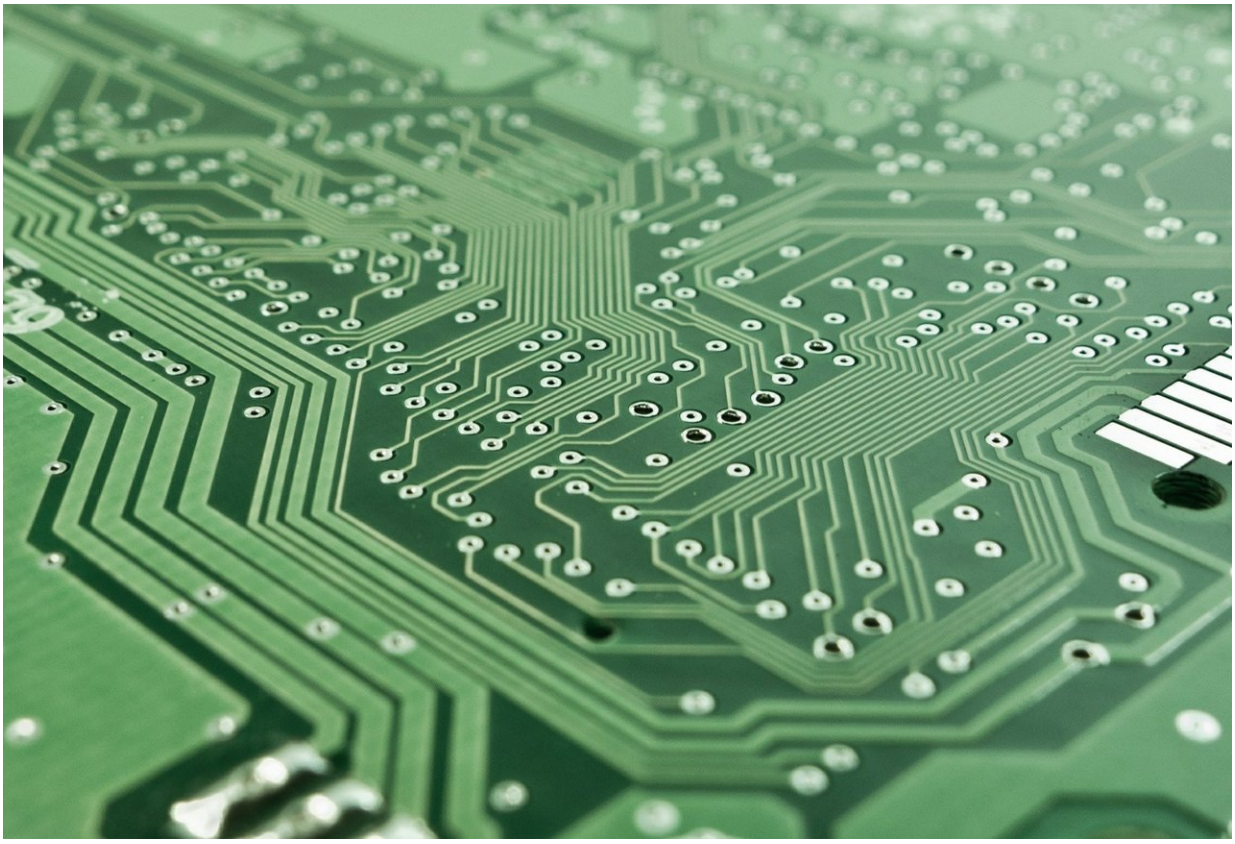
Chip-level vulnerabilities suggest risk of access point attacks

November 5 2018, by Nancy Owano



Credit: CC0 Public Domain

A pair of new Bluetooth security flaws expose wireless access points to attack. Well, that's worth a look as flaws in chips for connections include use in hospitals.

Armis, a security company, said, "medical centers use BLE to track the location of beacons on valuable assets like resuscitation carts. Retailers use BLE for point of sales devices, as well as indoor navigation applications. BLE is also used in new smart locks used by hotel chains, offices, and smart homes; even in cars."

BLEEDINGBIT is the name of two vulnerabilities—which its research spotters said were critical—related to Texas Instruments Bluetooth Low Energy chips embedded in Cisco, Meraki and Aruba access points.

Concern was voiced by the security researchers at Palo Alto-based Armis over not only devices but also access points delivering Wi-Fi to enterprise networks. Armis stated that it reported the issues to Texas Instruments and others affected.

Armis research said, "These proximity-based vulnerabilities allow an unauthenticated attacker to break into enterprise networks undetected. Once an attacker takes control over an access point, he can move laterally between network segments, and create a bridge between them—effectively breaking network segmentation."

Bradley Barth, *SC Media*, said Armis disclosed details of its findings on Nov .1, in conjunction with the CERT/CC at Carnegie Mellon University, which released its own security advisory.

Zack Whittaker, *TechCrunch*, pointed out the technically local—"in that a would-be attacker can't exploit the flaws over the internet and would have to be within Bluetooth range. In most cases, that's about 100 meters or so—longer with a directional antenna—so anyone sitting outside an office building in their car could feasibly target an affected device."

Dan Goodin, *Ars Technica*, said the access points "sold by Cisco, Meraki, and Aruba" had two critical vulnerabilities being patched that

could allow hackers to run malware inside the sensitive networks using the gear.

Lucian Constantin, *Security Boulevard*: "These vendors account for the majority of access points used in enterprises, but only APs that contain one of the affected BLE radio chips and have it turned on are affected."

The BLE protocol —based on the established Bluetooth protocol— is described by Palo Alto-based Armis as "relatively new" but going "much further by creating closely knit networks and enabling many of the novel uses of IoT devices." Alfred Ng in CNET explained their affinity with iOT devices. "BLE is a different standard from Bluetooth. First introduced in 2011 as Bluetooth 4.0, it boasts a much longer battery life than its predecessor. Because of that longevity, BLE chips are more likely to be used in IoT devices and medical devices."

Armis talked about network devices today. They said network devices were "an extremely valuable prize for hackers"—access to information with little defenses.

"While PCs and mobile platforms have well founded operating systems (OSs) which include inherent mitigations, network devices have only a limited OS if any, with very little mitigations in place."

Armis declared that "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." Armis has provided an ample collection of detailed information on all this, including technical overview and list of affected devices and affected access points, along with their disclosure process.

Armis said it plans to release a white paper about this issue at the Black Hat Europe conference in December. In their talk, Dor Zusman and Ben

Seri are to demo vulnerabilities.

The company has stated its mission, "to eliminate the IoT security blind spot."

Information about confirmations of bugs and the timing of patches are available on numerous sites at the time of this writing, including *Ars Technica*, *TechCrunch* and *The Register*.

For more details on Cisco' s responses, Goodin provided several links to Cisco's documentation on the vulnerabilities.

What does Armis recommend you do?

"For the first vulnerability, Armis Labs recommends updating your devices to the latest Texas Instruments version," reported Alfred Ng in CNET. For the second vulnerability, the researchers said to stop using Over Air Download, which is an optional feature.

Armis said in its report that they advised visiting the CERT/CC advisory page for the latest information.

More information: armis.com/bleedingbit/

Citation: Chip-level vulnerabilities suggest risk of access point attacks (2018, November 5) retrieved 25 April 2024 from https://techxplore.com/news/2018-11-chip-level-vulnerabilities-access.html