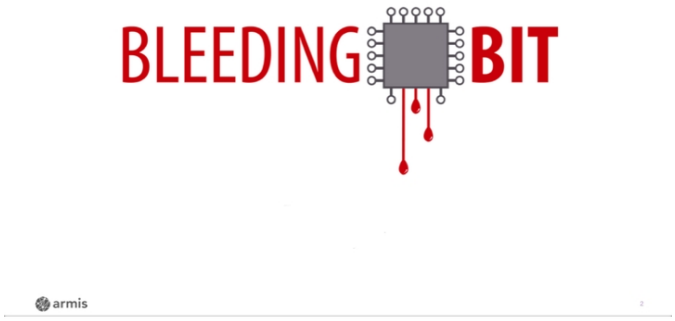
Written by Alice Marshall
02 November 2018

Wireless access points from multiple vendors pose the risk of two severe vulnerabilities dubbed Bleedingbit, IoT security firm Armis warns-- both providing attackers means to sneak into enterprise networks undetected.



The Bleedingbit flaws are found in Texas Instruments Bluetooth Low Energy (BLE) chips used Cisco, Meraki and Aruba wifi APs. Neither vulnerability can be detected or stopped by traditional network and endpoint security solutions, and if exploited they allow attackers to break into a network, take over access points, spread malware and move laterally across network segments.

The first Bleedingbit vulnerability triggers memory corruption in the TI BLE chips (cc2640, cc2650) embedded in Cisco and Meraki wifi APs, leading to compromise of the main system of the AP. The second issue impacts Aruba series 300 wifi APs with TI BLE chip (cc2540), and provides a backdoor for attackers to install new firmware, leading to a foothold in a secure network.

Armis alerted the companies in question before issuing the public warning of the Bleedingbit vulnerability, and as such companies are already working on solutions. TI should have a software update addressing the first vulnerability, while Cisco, Meraki and Aruba are working on patches. In turn, Armis is still working out the full reach of Bleedingbit vulnerabilities, and is working with CERT Coordination Centre (CERT/CC) and various vendors to validate the appropriate patches.

"In this instance, we have clearly identified how Bleedingbit impacts network devices," Armis adds. "But this exposure potentially goes beyond access points, as these chips are used in many other types of devices and equipment. They are used in a variety of industries such as

healthcare, industrial, automotive, retail, and more. As we add more connected devices taking advantage of new protocols like BLE, we see the risk landscape grow with it."

When it comes to protection from Bleedingbit, organisations using Cisco, Meraki and Aruba APs should check for the latest updates. OEMs using the TI chips should upgrade to the latest BLE-STACK.

Go Armis Discovers "Bleedingbit," Two Critical Chip-Level Vulnerabilities That Expose Millions of Enterprise Access Points to Undetectable Attack