computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-028

BLEEDINGBIT - Vulnerabilities Affecting Enterprise WiFi Devices

November 05, 2018 — v1.0

History:

- *05/11/2018 — v1.0 – Initial publication*

Summary

Security researchers disclosed details about two critical vulnerabilities related to the use of BLE (Bluetooth Low Energy) chips made by Texas Instruments (TI). The vulnerable BLE chips are embedded in WiFi network equipment from Cisco, Meraki and Aruba Networks [1]. Dubbed BleedingBit, the two vulnerabilities could allow remote attackers to execute arbitrary code and take full control of vulnerable devices without authentication.

Technical Details

The first vulnerability – CVE-2018-16986 – is a Remote Code Execution (RCE) vulnerability. Attackers can send multiple benign BLE broadcast messages, called *advertising packets*, which are stored in the memory of the vulnerable chip. As long as BLE is enabled on the target device, those packets – which contain hidden malicious code to be invoked later on – can be used together with an overflow packet to trigger an overflow of critical memory. When exploited, attackers are able to trigger memory corruption in the BLE stack of the chip, remotely executing malicious code [2].

The second vulnerability, identified as CVE-2018-7080, is basically a leftover development backdoor tool. That backdoor helps during the development stage to push over-the-air downloads (OAD) of the firmware. The function is intended for updating the devices remotely by connecting to them with a preset password.

Products Affected

The vulnerable chips are typically found in access points that provide WiFi service. They are also present in medical devices (insulin pumps, pacemakers), smart locks and a variety of other types of products that rely on Bluetooth Low Energy (BLE) technology for communication.

Devices Affected by the RCE Vulnerability (CVE-2018-16986)

The security vulnerability CVE-2018-16986 is present in these TI chips, when scanning is used (e.g., observer role or central role that performs scanning) in the following device/software combinations:

- CC2640 (non-R2) with BLE-STACK version 2.2.1 or an earlier version; or
- CC2650 with BLE-STACK version 2.2.1 or an earlier version; or
- CC2640R2F with SimpleLink CC2640R2 SDK version 1.00.00.22 (BLE-STACK 3.0.0); or
- CC1350 with SimpleLink CC13x0 SDK version 2.20.00.38 (BLE-STACK 2.3.3) or an earlier version.

Affected Access Points

Cisco APs (RCE vulnerability):

- Cisco 1800i Aironet Access Points
- Cisco 1810 Aironet Access Points
- Cisco 1815i Aironet Access Points
- Cisco 1815m Aironet Access Points
- Cisco 1815w Aironet Access Points
- Cisco 4800 Aironet Access Points
- Cisco 1540 Aironet Series Outdoor Access Point

Meraki APs (RCE vulnerability):

- Meraki MR30H AP
- Meraki MR33 AP
- Meraki MR42E AP
- Meraki MR53E AP
- Meraki MR74

Devices Affected by the Backdoor Vulnerability (CVE-2018-7080)

The vulnerability for CVE-2018-7080 affects any of the following TI's BLE chips provided the vendor choose to include the OAD feature in his device.

- cc2642r
- cc2640r2
- cc2640
- cc2650
- cc2540
- cc2541

Affected Access Points

- AP-3xx and IAP-3xx series access points
- AP-203R
- AP-203RP
- ArubaOS 6.4.4.x prior to 6.4.4.20
- ArubaOS 6.5.3.x prior to 6.5.3.9

- ArubaOS 6.5.4.x prior to 6.5.4.9
- ArubaOS 8.x prior to 8.2.2.2
- ArubaOS 8.3.x prior to 8.3.0.4

Aside from the devices listed above, the researchers are not aware of any other networking equipment that is affected. They advise visiting the CERT/CC advisory page for the latest information [3].

Recommendations

Apply the recommendation from vendors [4, 5].

References

[1] https://armis.com/bleedingbit/

[2] https://thehackernews.com/2018/11/bluetooth-chip-hacking.html

[3] https://www.kb.cert.org/vuls/id/317277

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181101-ap

[5] https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2018-006.txt