HMSSAR-2017-10-23-001

Publication date: 23 October, 2017
Last update: 23 October, 2017

HMS statement regarding BlueBorne

Overview

Research company Armis has recently reported about vulnerabilities in some Bluetooth stack implementations. The case, dubbed BlueBorne, does not reflect an issue with the Bluetooth standard or specification. On the contrary, it is a demonstration of implementation issues in some of the commonly available Bluetooth stacks. Furthermore, it is not a question of a single attack method used to hack all the affected stacks. BlueBorne is a set of different methods, where each attack is targeting a known vulnerability in the specific stack.

Impact

Anybus Wireless stand-alone modules do not use any of the stacks reported to be affected. Note also that the reported issues in BlueBorne are only related to Bluetooth BR/EDR and are not affecting Bluetooth Low Energy.

The Anybus Wireless modules has been analyzed and the conclusion is that the products do not contain the vulnerabilities taken advantage of in the BlueBorne case.

Referenced products and versions

- Anybus Wireless Bridge/EPA Bluetooth Client (legacy)
- Anybus Wireless Bridge/EPA Bluetooth Access Point (legacy)
- Anybus Wireless Bridge II
- Anybus Wireless Bolt

Severity / CVSS Score

-

HMS Recommendations

No action needed

Product updates

No updated needed

Additional information

https://www.armis.com/blueborne/