HMS information regarding the BrakTooth vulnerability

Overview

BrakTooth is a family of new security vulnerabilities in commercial BT stacks that range from denial of service (DoS) via firmware crashes and deadlocks in commodity hardware to arbitrary code execution (ACE) in certain IoTs. A total of 16 new security vulnerabilities have been discovered, with 20 common vulnerability exposures (CVEs) already assigned and four (4) vulnerabilities are pending CVE assignment from Intel and Qualcomm.

Referenced products

- Anybus Wireless Bridge II all variants
- Anybus Wireless Bolt Ethernet, Serial and CAN

Severity / CVSS Score

CVE-2021-34149; Base Score: 6.5 MEDIUM (https://nvd.nist.gov/vuln/detail/CVE-2021-34149)

Note; The Bolt and Bridge products contains a different Texas Instruments chip than referenced in this CVE, but it is assumed that the used chip behaves similarly.

HMS Recommendations

Make sure the device is using firmware version 2.00.12 or later. All firmware’s later than version 2.00.12 contains a prevention mechanism for a deadlock scenario also avoiding need for user action.

Product updates

Update to a firmware with version 2.00.12 or later.
Firmware can be downloaded from www.anybus.com/technical-support/support-home

Additional information

Online disclosure: https://asset-group.github.io/disclosures/braktooth/