HC3: Analyst Note

September 23, 2021 TLP: White Report: 202109231215

BrakTooth's Global Bite

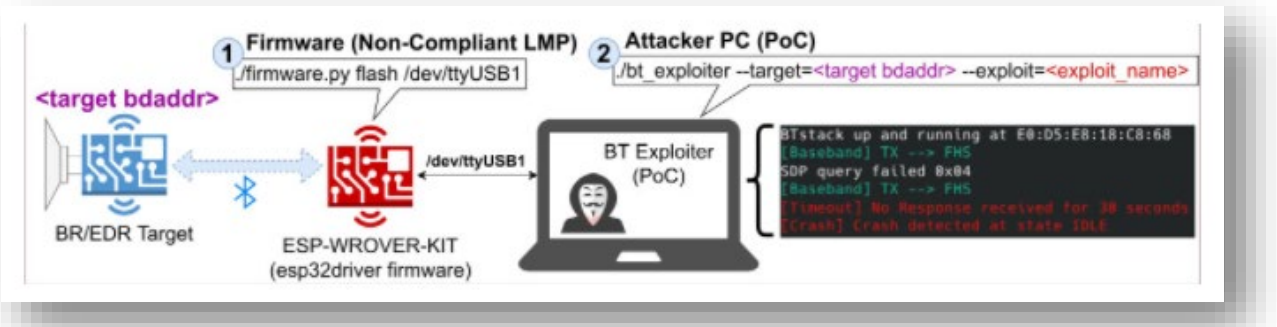
Executive Summary

The BrakTooth vulnerabilities came on the radar in August 31, 2021, after being discovered by the ASSET (Automated Systems Security) Research Group at the Singapore University of Technology and Design (SUTD). It is described as a new family of security vulnerabilities found in commercial Bluetooth Classic stacks for various System-on-Chips (SoC). BrakTooth, uses the Bluetooth Classic (BR/EDR) protocol and affects millions of Bluetooth-enabled devices that are manufactured by Intel, Qualcomm, Texas Instruments, Infineon (Cypress), Zhuhai Jieli Technology, and Silicon Labs.

This is a concern to the US Healthcare industry because Bluetooth devices are used in various essential roles and tampering with these devices could result in adverse consequences.

Report

BrakTooth vulnerabilities pose a threat to Healthcare and Public Health (HPH) sector because researchers say that the risk associated with the BrakTooth set of security flaws ranges from denial-of-service (DoS) by crashing the device firmware, or a deadlock condition where Bluetooth communication is no longer possible, to arbitrary code. This is a new family of security vulnerabilities, affecting Bluetooth stacks implemented on system-on-a-chip (SoC) circuits.



(Courtesy of Bleeping Computer)

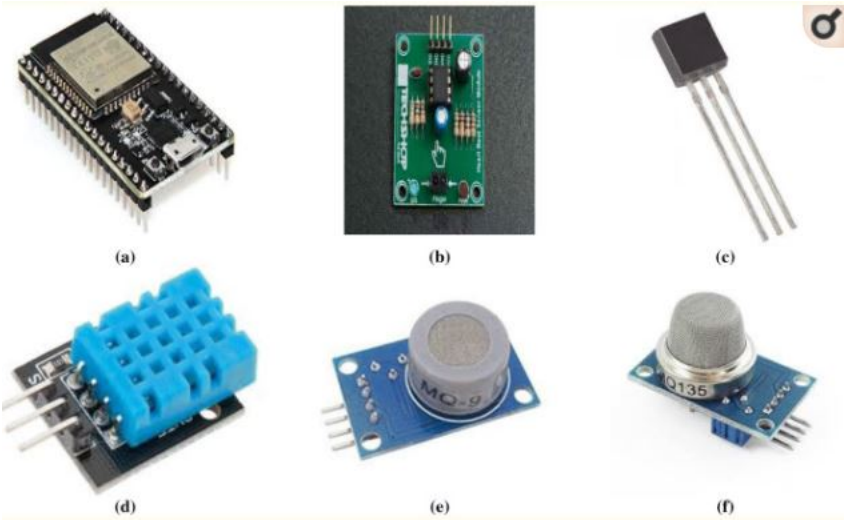
To exploit the vulnerability a threat actor will need an ESP32 development kit, a custom Link Manager Protocol (LMP) firmware, and a computer to run the proof-of-concept (PoC) tool.
The vulnerabilities in the BrakTooth collection target the LMP and baseband layers. Currently, they've been assigned 20 identifiers with a few more pending, and refer to the following 16 issues:

1) Feature Pages Execution (CVE-2021-28139 - arbitrary code execution/deadlock)
2) Truncated SCO Link Request (CVE-2021-34144 - deadlock)
3) Duplicated IOCAP (CVE-2021-28136 - crash)
4) Feature Response Flooding (CVE-2021-28135, CVE-2021-28155, CVE-2021-31717 - crash)
5) LMP Auto Rate Overflow (CVE-2021-31609, CVE-2021-31612 - crash)
6) LMP 2-DH1 Overflow (pending CVE - deadlock)
7) LMP DM1 Overflow (CVE-2021-34150 - deadlock)
8) Truncated LMP Accepted (CVE-2021-31613 - crash)

9) Invalid Setup Complete (CVE-2021-31611 - deadlock)
10) Host Conn. Flooding (CVE-2021-31785 - deadlock)
11) Same Host Connection (CVE-2021-31786 - deadlock)
12) AU Rand Flooding (CVE-2021-31610, CVE-2021-34149, CVE-2021-34146, CVE-2021-34143 - crash/deadlock)
13) Invalid Max Slot Type (CVE-2021-34145 - crash)
14) Max Slot Length Overflow (CVE-2021-34148 - crash)
15) Invalid Timing Accuracy (CVE-2021-34147 and two more pending CVEs - crash)
16) Paging Scan Deadlock (pending CVE - deadlock)

ESP32 is a chip developed by Espressif Systems known for packing a "powerful punch." Due to its small size, low power consumption, and low cost, it is used in a number of IoT applications including industrial equipment and medical devices. Based on the broad use of Bluetooth Classic, it is likely that some medical devices could be impacted by these vulnerabilities.

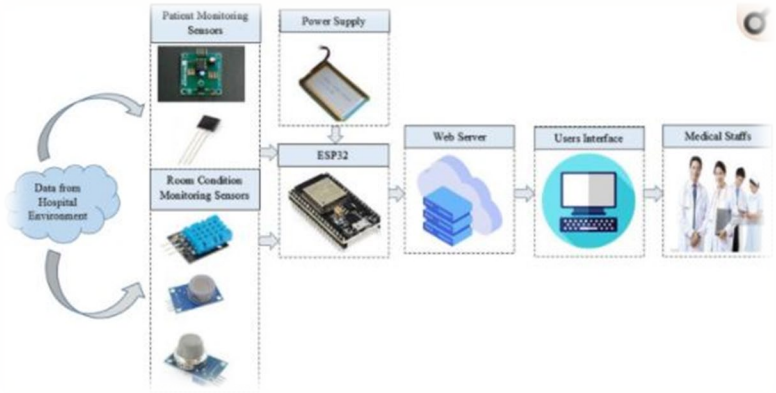
One of the uses for ESP32 is healthcare monitoring systems. In the two images below (Courtesy of NCBI) you will see the following ESP32 hardware components and its role in healthcare: **a)** ESP32 **b)** heart beat sensor **c)** body temperature sensor **d)** room temperature sensor **e)** CO sensor **f)** CO2 sensor.



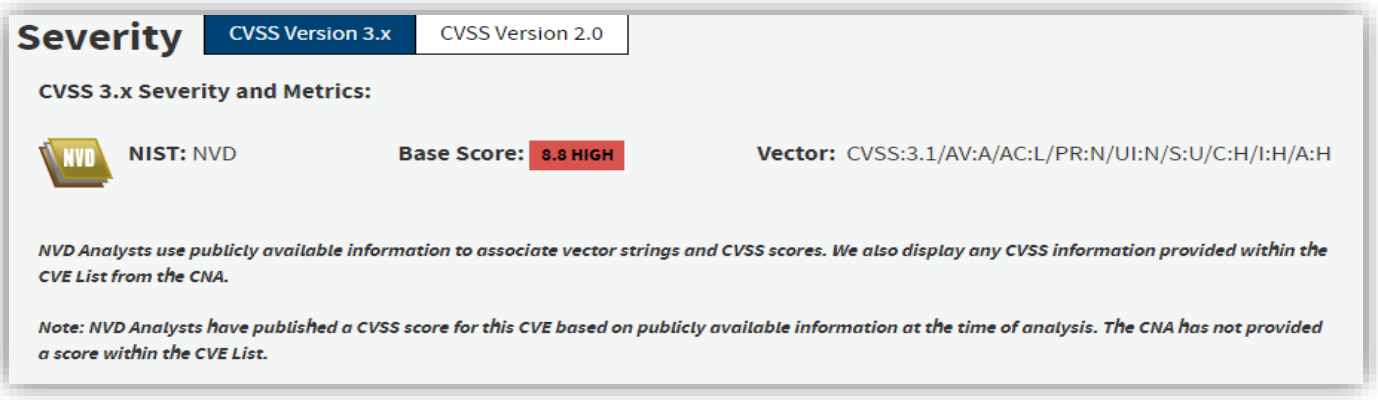
Below you can see the overall system architecture of healthcare monitoring systems with ESP32 in the center of it.

HC3: Analyst Note

September 23, 2021 TLP: White Report: 202109231215



When Intel and Qualcomm's WCN3990 SoC devices running on the AX200 SoC send a malformed packet it triggers a DoS response. The list of products impacted includes laptops and desktops from Dell (Optiplex, Alienware), Microsoft Surface devices (Go 2, Pro 7, Book 3), and smartphones (i.e., Pocophone F1, Oppo Reno 5G).



According to researchers, if any of the 16 vulnerabilities identified were successfully exploited, it would provide a remote threat actor or hacker the ability to launch multiple attacks, including Denial of Service (DoS), Arbitrary Code Execution (ACE), deadlocking, and firmware crashes on vulnerable devices. An attack of this nature against the Healthcare Industry could cause a multitude of impacts. There has yet to be any known instances of these attacks being successfully deployed against real world targets. Internationally, Singapore's Health Sciences Authority (HSA) published an advisory warning stakeholders' about how BrakTooth is can impact medical devices that utilize certain Bluetooth Link Manager Protocols. It is important to note, that these researchers are the first to make these claims and HC3 will continue to look for additional reports or data to confirm these claims.

The set of issues caused by a BrakTooth attack impacts a wide variety of devices, from consumer electronics to industrial equipment. The associated risk ranges from denial-of-service, deadlock condition of the device to arbitrary code execution. This vulnerability is believed to impacted billions of devices globally. Researchers also found that some devices displayed anomalous behavior that deviates from the Bluetooth Core Specifications. The summary of

vulnerabilities, anomalies, devices, and patch status are outlined in Table 1 below. (Courtesy of ISC)

SoC/Module Vendor	Bluetooth SoC	Firmware/SDK Version	CVE/Anomaly (A)	Patch Status
Espressif Systems	ESP32	esp-idf-4.4	CVE-2021-28135 CVE-2021-28136 CVE-2021-28139 A1: Accepts lower Link Manager Protocol (LMP) length	Available
Infineon (Cypress)	CYW20735B1	WICED SDK 2.9.0	CVE-2021-34145 CVE-2021-34146 CVE-2021-34147 CVE-2021-34148 A2: Accepts higher LMP length A6: Ignore encryption stop	Available*
Bluetrum Technology	AB5301A	Unspecified (LMP Subver. 3)	CVE-2021-34150 CVE-2021-31610 A1: Accepts lower LMP length A2: Accepts higher LMP length	Available*
Intel	AX200	Linux - ibt-12-16.ddc Windows - 22.40.0	2 CVE IDs pending A1: Accepts lower LMP length A2: Accepts higher LMP length A5: Invalid Response	Patch in progress
Qualcomm	WCN3990	crbtfw21.tlv, patch 0x0002	1 CVE ID pending A1: Accepts lower LMP length A2: Accepts higher LMP length A4: Ignore Role Switch Reject	Patch in progress
Zhuhai Jieli Technology	AC6366C	fw-AC63_BT_SDK 0.9.0	CVE-2021-34143 CVE-2021-34144 A1: Accepts lower LMP length A2: Accepts higher LMP length	Patch in progress
Zhuhai Jieli Technology	AC6925C	Unspecified (LMP Subver. 12576)	CVE-2021-31611 CVE-2021-31613 A1: Accepts lower LMP length A2: Accepts higher LMP length	Investigation in progress

HC3: Analyst Note

September 23, 2021 TLP: White Report: 202109231215

SoC/Module Vendor	Bluetooth SoC	Firmware/SDK Version	CVE/Anomaly (A)	Patch Status
Zhuhai Jieli Technology	AC6905X	Unspecified (LMP Subver. 12576)	CVE-2021-31611 CVE-2021-31612 CVE-2021-31613 A1: Accepts lower LMP length A2: Accepts higher LMP length	Investigation in progress
Actions Technology	ATS281X	Unspecified (LMP Subver. 5200)	CVE-2021-31717 CVE-2021-31785 CVE-2021-31786 A1: Accepts lower LMP length A2: Accepts higher LMP length	Investigation in progress
Harman International	JX25X	Unspecified (LMP Subver. 5063)	CVE-2021-28155 A1: Accepts lower LMP length A2: Accepts higher LMP length	Pending
Silabs	WT32i	iWRAP 6.3.0 build 1149	CVE-2021-31609 A1: Accepts lower LMP length A2: Accepts higher LMP length	Pending
Qualcomm	CSR8811/ CSR8510	v9.1.12.14	1 CVE ID pending A1: Accepts lower LMP length A2: Accepts higher LMP length	No fix
Texas Instruments	CC2564C	cc256xc_bt_sp_v1.4	CVE-2021-34149 A1: Accepts lower LMP length A2: Accepts higher LMP length	No fix

Table 1: *Patch Status, Vulnerabilities and SDK/Firmware Version of Affected Devices (*Contact vendor to acquire patch)*

Patch Status Key:

Available: The vendor has replicated the vulnerability and a patch is available.
Patch in progress: The vendor has successfully replicated the vulnerability and a patch will be available soon.
Investigation in progress: The vendor is currently investigating the security issue and is being assisted by the researchers.
Pending: The vendor hardly communicated with the researchers and the status of their investigation is unclear at best.
No fix: The vendor has successfully replicated the issue, but there is no plan to release a patch.

Additionally, researchers found that more than 1,400 product listings are affected by BrakTooth. Some of these devices are:

- Smartphones
- BT enabled keyboards and toys
- Infotainment systems
- Laptop and desktop systems
- Audio devices (speakers, headphones)
- Home entertainment systems
- Keyboards
- Toys
- Industrial equipment (i.e., programmable logic controllers – PLCs)

Mitigation

To mitigate the BrakTooth threat the following is recommended:

- An audit of the devices/components in use is recommended to help stakeholders that may be uncertain about the extent of Bluetooth usage and associated devices. A risk assessment should be conducted to efficiently assess BrakTooth's risk to users or day-to-day operations. With the potential magnitude of this attack vector, enhanced physical security could be an interim measure to reduce the likelihood of an attack while affected devices are patched/replaced.

- It is recommended that users and administrators work with any identified affected manufacturers to receive validated patches and coordinate with vendors to get a timeline for vulnerabilities that do not have a patch. It is recommended for end users, to check if their Bluetooth products are currently being used are in Table 1 (above).

- If there is not a patch to apply immediately or the patch is "in progress" or if the vendor is "still investigating," monitor the device for any anomalous behavior. If the device is unable to be reached then there could be an issue.

- The BrakTooth vulnerability is based on implementations of the Bluetooth Classic protocol, therefore the threat actor must be within the radio range of the target to execute the attack.

It is recommended that Healthcare Delivery Organizations (HDOs), Healthcare Professionals and manufacturers reach out to the ISAC/ISAOs for assistance with responding.

The ASSET Group Research team has a request form (*https://poc.braktooth.com)* online until October 31, 2021 for Bluetooth semiconductor/module/OEM vendors as well as researchers to fill out to receive a link to the BrakTooth PoC tool and instructions for running the exploits.

Analyst Comment

The potential risks associated with the BrakTooth set of security vulnerabilities range from arbitrary code and denial-of-service (DoS) by crashing the device firmware to deadlock condition where Bluetooth communication is no longer possible. An attack like this could cause impacts for the Healthcare industry ranging from a data breach to a system lockdown, potentially preventing a patient from receiving treatment.

A risk assessment should be conducted to efficiently assess BrakTooth's risk to users or day-to-day operations. With the potential magnitude of this attack vector, enhanced physical security could be an interim measure to reduce the likelihood of an attack while affected devices are mitigated. In addition to this, if patches from affected medical device manufacturers are not currently available, the patch is listed as "in progress" from the chip manufacturer, or if the chip manufacturer is "still investigating," it is recommended that company CISOs monitor the device for any anomalous behavior and work with medical device manufacturers on recommended compensating controls. Researchers say Bluetooth (BT) stack is often shared across many products; therefore, other products are affected by BrakTooth.

References

Barrett, Brian. "Security News This Week: BrakTooth Flaws Affect Billions of Bluetooth Devices," Wired. 4 September 2021. https://www.wired.com/story/BrakTooth-bluetooth-whatsapp-fine-omg-cable/

Cimpanu, Catalin. "Billions of devices impacted by new BrakTooth Bluetooth vulnerabilities," The Record by Recorded Future. 1 September 2021. https://therecord.media/billions-of-devices-impacted-by-new-BrakTooth-bluetooth-vulnerabilities/

Cisomag." Millions of Bluetooth Devices Affected by BrakTooth Flaws." 9 September 2021.https://cisomag.eccouncil.org/millions-of-bluetooth-devices-affected-by-BrakTooth-flawsGarbelini, Matheus E.; Chattopadhyay, Sudipta; Bedi, Vaibhav; Sun, Sumei; Kurniawan, Ernest. "BRAKTOOTH: Causing Havoc on Bluetooth Link Manager," Asset-Group. https://asset-group.github.io/disclosures/BrakTooth/

Hubschmann,Ida. "ESP32 for IoT: A Complete Guide," Nabto. 28 August 2020. https://www.nabto.com/guide-to-iot-esp-32/

Ilascu, Ionut. "Bluetooth BrakTooth bugs could affect billions of devices," Bleeping Computer. 2 September 2021. https://www.bleepingcomputer.com/news/security/bluetooth-BrakTooth-bugs-could-affect-billions-of-devices/

Islam, Md. Milon;Rahaman, Ashikur; Islam, Md. Rashedul. "Development of Smart Healthcare Monitoring System in IoT Environment," National Center for Biotechnology Information. 26 May 2020. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7250268/

NIST, ITL. "CVE-2021-28139 Detail," National Vulnerability Database. 7 September 2021. https://nvd.nist.gov/vuln/detail/CVE-2021-28139

Riley, Duncan. "BrakTooth Bluetooth vulnerabilities could affect billions of devices," Silicon Angle. 6 September 2021. https://siliconangle.com/2021/09/06/BrakTooth-bluetooth-vulnerabilities-affect-billions-devices/

Then, Satsuki. "BrakTooth vulnerability impacts Bluetooth devices," Slash Gear. 7 September 2021. https://www.slashgear.com/BrakTooth-vulnerability-impacts-bluetooth-devices-07689900/

Tok, Yee Ching. "BrakTooth: Impacts, Implications and Next Steps," InfoSec Handlers Diary Blog. 31 August 2021. https://isc.sans.edu/diary/BrakTooth%3A+Impacts%2C+Implications+and+Next+Steps/27802

Westerman,Soren; Bendorff Fallesen, Jesoer; Trock,Martin. "IoT in hearing aids with Nabto technology," Nabto. 9 November 2020. https://www.nabto.com/cases/widex/

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback