Bluetooth devices proven to be vulnerable to unfixable security problems

September 1 2021

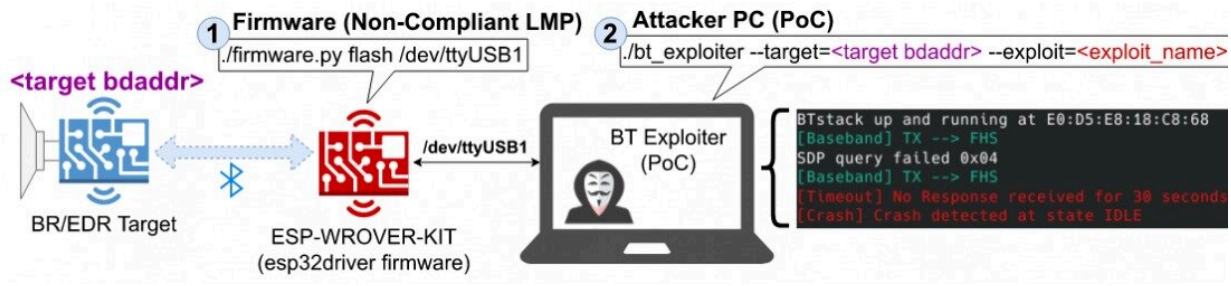

Illustration of a BrakTooth attack scenario. Credit: SUTD

Researchers from the Singapore University of Technology and Design (SUTD) released 16 new security vulnerabilities, with the codename BrakTooth, affecting a wide range of Bluetooth classic (BR/EDR) implementations. The report, done in collaboration with the Institute for Infocomm Research (I2R), Agency for Science, Technology and Research (A*STAR), was led by Assistant Professor Sudipta Chattopadhyay from SUTD's ASSET (Automated Systems SEcuriTy) Research Group.

In the white paper titled "BrakTooth: Causing Havoc on Bluetooth Link Manager," it was noted that the vulnerabilities affected major Bluetooth chipset vendors including Intel, Qualcomm, Texas Instruments, Infineon (Cypress) and Silicon Labs. The scope of these vulnerabilities are likely

to affect mostly mainstream electronic device users due to their heavy usage of laptops and smartphones in their day-to-day life. More specifically, major laptop vendors from Microsoft, Asus, Dell, and HP etc. are using the affected Intel chipset (Intel AX200). Concurrently, the affected Qualcomm chipsets (WCN3990/8) are used by major smartphones and tablet vendors such as Samsung, Sony and Xiaomi.

The research team has clarified that the reported vulnerabilities allow an attacker to remotely shut down a Bluetooth enabled device. For example, certain vulnerabilities allow an attacker to remotely shutdown a headset or speaker. This means when a user is listening to audio from a laptop using the headset or speaker, they can experience the audio being cut abruptly. The attacks can be launched continuously, which, in turn can impair the user's listening experience.

The most serious vulnerability reported by the research team allows for arbitrary code execution in an embedded controller. An arbitrary code execution allows an attacker to remotely execute attacker chosen code in the target device. For example, the reported vulnerability allows the attacker to remotely delete all data in the target devices' memory. Apart from affecting most major laptops, smartphones and tablets, the vulnerabilities also impact a range of other products for instance, the industry automation, automotive infotainment systems, aircraft entertainment systems, speakers and headsets etc.

The research team also highlighted that the Bluetooth listing reports over 1,400 products to be affected. However, due to the limited search capability in the Bluetooth listing website, the actual number of affected products is expected to be an order of magnitude higher than the number of listings observed.

Researchers of the reported vulnerabilities followed a responsible disclosure process while reporting the vulnerabilities to vendors. They

provided all Bluetooth system-on-chip (SoC) and module vendors at least 90 days until the public disclosure to fix the vulnerabilities in their chipsets. However, researchers have reported that patches for these vulnerabilities are only partially available for now.

For instance, patches for Intel and Qualcomm will only be available around October 2021. Thus, several major laptops and smartphones will be unpatched until the fixes are available from Intel and Qualcomm. Researchers also warned that several of these vulnerabilities, as reported by the respective vendors such as Qualcomm, are impossible to fix due to the unavailability of space in the affected chipsets. Thus, any module/product employing such chipsets are likely to remain vulnerable forever. Researchers advise Bluetooth product vendors to conduct a thorough risk assessment if their product is using certain vulnerable chipsets and reconsider their design if the risk is not acceptable.

The research team understands the risk in releasing the attack code (exploits) as many devices remain vulnerable to BrakTooth attacks as of today. However, any Bluetooth SoC and module vendors can get access to the attack code to evaluate the security of their device here: poc.braktooth.com .

Provided by Singapore University of Technology and Design