New series of Bluetooth vulnerabilities discovered that could put millions of Windows and Android devices worldwide in trouble

Hackers can easily take advantage of existing vulnerabilities in the Bluetooth protocol to deploy many different violating activities.

Bluetooth is a connection technology that has appeared for a long time and is probably no stranger to each of us. Bluetooth connectivity makes it easy to move files, photos, and documents between technology devices, as well as connect and exchange data between a main device and peripheral devices within a certain distance.

But besides the undisputed convenience, this connectivity technology has inadvertently raised issues of data security and privacy at the individual level. Hackers can easily take advantage of existing vulnerabilities in the Bluetooth protocol to deploy many different violating activities.

Recently, a 'collection' of security vulnerabilities has been discovered to exist in many Bluetooth chipset systems being equipped on products of a series of popular OEM SoCs. The list includes Intel, Qualcomm, Texas Instruments, Infineon (Cypress), Silicon Labs and many big names. Therefore, the number of affected devices worldwide will be extremely large, difficult to measure accurately.

This series of security vulnerabilities is called BrakTooth, and was first discovered by a team of researchers from the Singapore University of Technology and Design, after analyzing 13 Bluetooth devices from the major SoC vendors mentioned above.

The impact from BrakTooth vulnerabilities is also varied. From damaging the target device using specially crafted Bluetooth Link Manager Protocol packets, to the most dangerous of arbitrary code execution (CVE-2021-28139).

According to preliminary investigation results, the BrakTooth vulnerabilities are confirmed to exist in the products of at least 11 manufacturers, but can affect 1,400 different Bluetooth chipsets. These chips are equipped on many popular technology products such as smartphones (Pocophone F1, Oppo Reno 5G.), laptops (Dell Optiplex, Alienware.), desktop computers (Dell Optiplex, Alienware.). Microsoft Surface Go 2, Pro 7, Book 3…), audio devices (speakers and headphones), home entertainment systems, and even toys.

Currently Expressif, Infineon and Bluetrum have released patches, while other OEMs are still actively investigating the issue.

While the patch has not been released, security vendors recommend that you temporarily limit Bluetooth use, and turn off Bluetooth connectivity when not in use.

Video demo of the BrakTooth vulnerability hacking process: