

CYBER GUIDANCE ISSUE 00220

‘BRAKTOOTH’ BLUETOOTH FLAWS AFFECTS BILLIONS

DATE ISSUED: 10th November 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

1,4000 chipsets are affected by the BrakTooth collection of flaws that are used in billions of devices including Smartphones, PCs, toys, industrial equipment and many more that rely on Bluetooth communication. It is now up to vendors to assess and release patches or workarounds.

BREAKDOWN

The embargo period for a Proof of Concept for the 22 vulnerabilities associated with BrakTooth is over and researchers from Singapore have released their findings – both the test kit and full exploit code on the BrakTooth GitHub site. Initially, BrakTooth consisted of 16 vulnerabilities, however, there have been many updates since the original papers publication. BrakTooth is known to affect iPhones, Microsoft Surface laptops, Dell PCs, Sony and Oppo smartphones and Panasonic audio equipment to name a few. CVEs are pending from Intel and Qualcomm. Patches began being released in September although some are still yet to be patched leaving devices vulnerable.

REMEDATION STEPS

- Apply the security patches provided by vendors that are relevant to your device and current installed version after appropriate testing has been completed.
- Organisations that allow the use of Bluetooth on their network should monitor for any anomalous behaviour
- Inform and educates users about the potential for compromise over Bluetooth services

REFERENCES & RESOURCES

Threatpost <https://threatpost.com/braktooth-bluetooth-bugs-exploit-poc/176036/>
GitHub https://github.com/Matheus-Garbelini/braktooth_esp32_bluetooth_classic_attacks
Malware Bytes <https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/09/braktooth-bluetooth-vulnerabilities-crash-all-the-devices/>
US CISA <https://us-cert.cisa.gov/ncas/current-activity/2021/11/04/braktooth-proof-concept-tool-demonstrates-bluetooth>
PC Mag <https://au.pcmag.com/security/89304/braktooth-vulnerabilities-affect-countless-bluetooth-devices>