New BlueBorne Attack puts Billions of Bluetooth Devices at Risk

Read full article
Learn World of Hacks @
fb.com/KnowCyberWorld/

KNOW
CYBER
WORLD

BlueBorne ?

BlueBorne is a series of vulnerabilities that enables an airborne attack which could be used by hackers to spread malware or intercept data

This BlueBorne vulnerabilities were discovered by IoT Security firm Armis, which first responsibly reported the flaws to the impacted vendors, including Google, Microsoft and the Linux community

This could occur via MITM cyberattacks without the need for any user interaction or clicks

The flaws impacted "all" devices on Android, Windows, Linux and Apple iOS versions pre-iOS 10, Armis said

WHY BlueBorne MAKES BLUETOOTH DEVICES SO VULNERABLE ?

BEFORE THAT LETS SEE ABOUT

BLUETOOTH

BLUETOOTH

Bluetooth is a widely used wireless communication protocol for exchanging data over short distances, is enabled on a target device. Unfortunately, it is often enabled by default on too many devices

Bluetooth enabled devices are constantly searching for incoming connections from any devices, and not only those they have been paired with.

This means a Bluetooth connection can be established without pairing the devices

This makes BlueBorne one of the most broad potential attacks found in recent years, and allows an attacker to strike completely undetected

These silent attacks are invisible to traditional security controls

THE VULNERABILITIES

You can surf with these security flaw numbers:

CVE-2017-1000251
CVE-2017-1000250
CVE-2017-0785
CVE-2017-0781
CVE-2017-0782
CVE-2017-0783
CVE-2017-8628
CVE-2017-14315