Billions of devices are affected by the new Bluetooth attack

On Tuesday, researchers at Armis Labs published details of a new attack that they thought could potentially affect all devices that could use Bluetooth.

On Tuesday, researchers at Armis Labs published details of a new attack that they thought could potentially affect all devices that could use Bluetooth.

Armis is the Internet of Things security company, calling this attack BlueBorne. It allows an attacker to completely control the device, access data and networks, infiltrate the Air-Gapped network which is said to be very good security, create a very wide botnet from IoT devices . It is also capable High infection and can transmit malware to nearby devices.

Armis said it affects computers running Windows and Linux as well as IoT devices and mobile devices running Android or iOS.

Bluetooth is one of the most popular wireless communication methods. This technology has been used by many devices in recent years as more and more mobile devices are available. Currently, there are nearly 5.3 million devices at risk.

Billions of devices using Bluetooth are likely to be attacked

Perhaps the most remarkable thing about BlueBorne is that the device does not need to access the website, download files or even connect to another device to become a victim. Just turn on Bluetooth, the hacker can take control. All is done without the user knowing.

Armis also announced eight related zero-day vulnerabilities, four of which are said to be very important. List of affected devices is available on the company's website.*https://www.armis.com/blueborne/#/devices* Armis said they contacted big companies like Google, Microsoft, Apple, Samsung and Linux to get the coordination.