Masterhacks – La compañía de ciberseguridad, Armis Labs, reveló recientemente la existencia de una vulnerabilidad en todos los dispositivos con tecnología Bluetooth.

Armis Labs estima que la cantidad de dispositivos infectados está entre los 5.3 mil millones que corren Windows, Linux, iOS y Android, y que pueden ser un teléfono celular, computadora portátil o de escritorio, wearables o cualquier dispositivo de IoT con Bluetooth.

La compañía nombró en su informe al nuevo vector de ataque como BlueBorne, y explica que aprovecharse de la vulnerabilidad no requiere que el usuario ingrese a un enlace malicioso, ni que descargue algún tipo de malware ni sincronizar por Bluetooth. Simplemente se requiere que la conectividad Bluetooth esté activa.

Los hackers pueden aprovecharse de BlueBorne para conectarse a cualquier dispositivo y tomar el control del mismo, para implantar un malware con el que pueden extraer información, convertir al dispositivo en parte de una botnet o infectar con ransomware. Se trata de hasta ocho vulnerabilidades zero-day que los atacantes pueden utilizar.

Armis Labs publicó una lista con los dispositivos potencialmente vulnerables, y contactó con los principales fabricantes de software y hardware para comenzar el desarrollo de parches de seguridad.