NCIS CYBER DIRECTORATE

Bluetooth Devices Provide an Additional Attack Vector for Malicious Cyber Actors

As more technologies that are used for communicating and storing information become Bluetooth-enabled, malicious cyber actors are finding new methods of conducting cyber attacks against these devices. Bluetooth is a wireless technology standard for exchanging data between fixed and mobile Bluetooth-enabled devices. The data is transferred over short distances using short-wavelength ultra-high frequency (UHF) radio waves, and does not require Internet access. Bluetooth capabilities are available in a variety of technologies to include personal electronic devices (PEDs) and wearables, vehicles, office equipment, and surveillance systems. Security researchers have discovered new vulnerabilities in Bluetooth devices that if exploited, could give malicious cyber actors access to the targeted device, devices connected to that device, or sensitive information such as personally identifiable information (PII) or locational data.

- In August 2019, a vulnerability known as Key Negotiation of Bluetooth (KNOB) was discovered and, if exploited, could allow a malicious cyber actor to monitor or manipulate traffic that is transferred between two devices that are paired via Bluetooth. The KNOB vulnerability is further described in CVE-2019-9506. To view the traffic, cyber actors exploit the vulnerability which, allows them to change the initial connection process by lowering the encryption level. Once the encryption level has been lowered, the actors could then enter the initial negotiation phase that takes place as the two devices try to establish a connection. This method of attack could be used to collect intelligence from devices such as smartphones, laptops, and other smart Internet of Things (IoT) devices.

- In July 2019, Boston University researchers discovered a way for cyber actors to track movements of Bluetooth Low Energy (BLE) devices running on various operating systems, including iOS, macOS, and Windows 10. BLE devices are those that use a low level of power to operate and do not exchange large amounts of data, such as smart watches, fitness devices, scanners, and other Bluetooth-enabled computer equipment to include a mouse or keyboard.

The potential damage to a device or amount of information available to hackers varies depending on the intended use of the Bluetooth-enabled device. For instance, damage could be greater to a device used for transmitting information and connecting to other devices, than it would be for a device used solely for audio. For Bluetooth attacks to be successful, the targeted devices must be Bluetooth-enabled and the Bluetooth feature must be turned on. Additionally, attackers need to be in close proximity to conduct an attack. The most effective way to mitigate a Bluetooth attack is to turn the Bluetooth function on a device to “OFF”, or set the Bluetooth visibility of a device to “OFF” when not in use to stop other devices from scanning and searching for your Bluetooth device.