SECRET

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 51) Aug 18**

1. **Introduction.** A highly **critical cryptographic** vulnerability has been found that affects **Bluetooth protocol** implementation. The vulnerability allows an **unauthenticated, remote attacker** in physical proximity of targeted devices to **intercept, monitor** or manipulate the **Bluetooth data communication.**

2. **Technical Details**

   a. The security vulnerability is related to following **Bluetooth features:-**

      (1) **Bluetooth low energy (LE)** implementations of Secure Connections Pairing in operating system.

      (2) **BR/ EDR** implementations of Secure Simple Pairing in device firmware.

   b. Vulnerability details are as under:-

      (1) **CVE Number -** CVE-2018-5383.

      (2) **Vulnerability Impact:** Bluetooth interception.

   c. A **remote attacker** within the range of targeted devices during the **pairing process** can launch a **man-in-the-middle attack** to obtain the cryptographic key used by the device, to **steal data** going over-the-air, and **inject malware.**

3. **Affected Products.** The Bluetooth vulnerability affects **firmware** or **operating system software drivers** from some following major vendors:-

   a. Apple

   b. Broadcom

   c. Intel

   d. Qualcomm

4. **Mitigation Measures**

   a. **Security Patches.**

      (1) The **Bluetooth SIG** has now updated the Bluetooth specification for products to **validate public keys** received as part of **public key-based** security procedures.

      (2) **Apple** and **Intel** have already released patches for this security vulnerability. Regularly **visit 'vendor websites (Broadcom, Qualcomm)** for remaining security patches.

   b. **Best Practices to Bluetooth**

      (1) Don't accept any unexpected Bluetooth Pairing requests.

      (2) Turnoff Bluetooth after use.

(3) Set device Visibility to "OFF".

(4) Always use a **security code** whenever pairing with another device.

(5) It is advised to use a minimum of eight characters in **PIN.**

5. **Recommendations.**

a. Strictly follow all **mitigation measures** mentioned at **pare 4.**

b. Keep **operating system** and all softwares **up to date.**