Security Advisory

VU #918987
CVE# 2019-9506

Marvell was notified of a specification vulnerability (CVE# 2019-9506) on the encryption Key Negotiation of Bluetooth (KNOB) BR/EDR which affects all Bluetooth devices regardless of vendor. More information on this issue and its remedy can be found at https://www.bluetooth.com/security/statement-key-negotiation-of-bluetooth/.

The attack occurs at the LMP link-layer and affects the controller establishing an encrypted BR/EDR link. If the host is attacked it will not be aware that an attack has been successfully mounted unless an application or host stack requests the encrypted key length and determines it is shorter than intended. BLE is not believed to be impacted by an analogous attack due to the current difficulty in brute forcing the encryption key with 56 bits of entropy.

Bluetooth Sig has adopted Erratum 11838 which addresses this fix. It applies to Bluetooth Core Specification versions 4.2 to 5.1 and includes a recommendation of a minimum encryption key length of 7 octets for encrypted BR/EDR connections. Bluetooth Sig will include testing for the new recommendation within its Bluetooth Qualification Program.

While there is low probability of exploitation on the affected systems (8887, 8897, 8977, 8987, and 8997), Marvell places the highest priority on addressing security concerns.

Marvell encourages customers to contact their Marvell representative for additional support.