TECHNICAL UPDATE ON WPA2/KRACK VULNERABILITY FOR SGX 5150

- **Description of KRACK Common Vulnerabilities and Exposures (CVE) Classes**
- **SGX 5150 KRACK Vulnerability and Release Information**
- WPA2 KRACK Security Vulnerability Update and FAQs

Description of KRACK Common Vulnerabilities and Exposures (CVE) Classes

A security researcher publicly disclosed a serious vulnerability in the WPA2 encryption protocol used to establish a secure Wi-Fi connection between the Wi-Fi Client and the Access Point (AP). The vulnerability is related to the key handshake between the Wi-Fi Client (Supplicant) and the Access Point (Authenticator) that derives and installs sessions keys. An attacker can trick the Wi-Fi client to reinstall an already-in-use key by manipulating and replaying the handshake messages.

The CVEs associated with the KRACK attack can be categorized into three groups.

GROUP 1:

- CVE-2017-13077
- CVE-2017-13078
- CVE-2017-13079

These CVEs describe a vulnerability with the re-installation of the pairwise security keys between an Access Point (AP) and a particular station (client) device. If the vulnerability exists, it exists in code that implements the security supplicant as defined in the 802.11 specification.

GROUP 2:

- CVE-2017-13080
- CVE-2017-13081

These CVEs describe a vulnerability with the re-installation of group security keys used for multicast and broadcast packets. The risk is less than that of the first set of CVEs as the attack only allows for duplication of network packets that were already sent. The upper layer protocols (TCP, UDP) will generally not have an issue with these duplicated packets.

GROUP 3:

- CVE-2017-13082
- CVE-2017-13084
- CVE-2017-13086
- CVE-2017-13087
- CVE-2017-13088

CVE-2017-13082 describes a vulnerability in Aps that implement the FT association requests available with 802.11r specification. The other CVEs describe vulnerabilities in station devices that implement the *PeerKey* handshake and other specific wireless network management exchanges.

SGX 5150 KRACK VULNERABILITY AND RELEASE INFORMATION

The table below provides information about how the SGX 5150 is affected by the 3 vulnerability groups and the release plan for addressing these vulnerabilities

Lantronix Current Product	Group 1	Group 2	Group 3	Release Status
SGX 5150	X	X	Not Affected	Available now