WPA2 KRACK Security Vulnerability

Official Laird Statement *DATE: 10/25/2017*

INTRODUCTION:

A flaw in the WPA2 security protocol has recently been discovered. The bug, known as “KRACK” for Key Reinstallation Attack, exposes a weakness in WPA2 which is one of the most popular security protocols used to encrypt most modern Wi-Fi connections.

Laird is aware of the industry wide vulnerability impacting WPA2 security and we are committed to providing our customers with patches and updates as quickly as possible.

DESCRIPTION OF VULNERABILITY:

Residing in WPA2’s four-way handshake, the flaw allows attackers to decrypt any data or information that is transmitted including sensitive information such as passwords, credit card numbers, emails and messages, photos, etc. The attack works on all modern protected Wi-Fi networks and affects most operating systems including Android, Linux, Apple, Windows, and more. Depending on the network configuration, attackers can even inject or manipulate data.

If your device supports Wi-Fi, it is most likely affected, however the attacker would have to be physically close to your device. Additionally, secure websites such as online banking and shopping are not compromised.

For additional resources, visit https://www.krackattacks.com.

Assigned CVE Identifiers

Details of the vulnerability are tracked by a number of Common Vulnerabilities and Exposures (CVEs). Below is the current list of CVEs as outlined in the original research report by Mathy Vanhoef of imec-DitriNet, KU Leuven.

- **CVE-2017-13077**: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
- **CVE-2017-13078**: Reinstallation of the group key (GTK) in the 4-way handshake.
- **CVE-2017-13079**: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
- **CVE-2017-13080**: Reinstallation of the group key (GTK) in the group key handshake.
- **CVE-2017-13081**: Reinstallation of the integrity group key (IGTK) in the group key handshake.
- **CVE-2017-13082**: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- **CVE-2017-13084**: Reinstallation of the STK key in the PeerKey handshake.
- **CVE-2017-13086**: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
- **CVE-2017-13087**: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

The information in this document is subject to change without notice.

- **CVE-2017-13088**: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

IMPACTED LAIRD PRODUCTS:

Laird is aware of the WPA2 vulnerability as outlined by Mathy Vanhoef of imec-DitriNet, KU Leuven. We put the security of our customers first and foremost and are testing all of our products for this vulnerability. We will provide patches and updates as they become available.

Current Products	Build Versions Impacted	
	Windows	Linux
60 Series (ST60-SiPT, ST60-2230C)	N/A	3.5.5.14 and earlier
50 Series (SSD50NBT, MSD50NBT, M2SD50NBT)	24.3.4.27 and earlier	3.5.4.20 and earlier
45 Series (SSD45N, MSD45N)	23.3.5.9 and earlier	3.5.4.20 and earlier
40 Series (SSD40NBT, MSD40NBT)	22.3.5.14 and earlier	3.4.1.1 and earlier
30 Series (SSD30AG, MSD30AG)	21.3.1.9 and earlier	N/A
15 Series (PE15N, EC25N)	NDIS6 = 3.4.18.0 and earlier NDIS5 = 3.4.12.7 and earlier	N/A
WB Products (WB50NBT, WB45NBT, WB40NBT)	N/A	3.5.4.20 and earlier
Sterling-LWB for Linux	N/A	3.5.5.18 and earlier
Sterling-LWB for WICED	N/A	WICED Studio 5.2.0 and earlier WICED Studio 4.1.2 and earlier
Sterling-LWB5	N/A	3.5.5.18 and earlier
TiWi5	N/A	Non-patched wpa_supplicant 2.6 or earlier
TiWi-C-W	N/A	WICED Studio 3.7.0-7 and earlier
TiWi-BLE	N/A	Non-patched wpa_supplicant 2.6 or earlier
RG1xx	N/A	93.7.1.13 and earlier

Note: Contact your Laird sales representative for information regarding EOL and Legacy products.

The information in this document is subject to change without notice.