Introduction

Cypress is aware and has analyzed the vulnerabilities associated with the recently released *KRACK* attack (https://www.krackattacks.com) against implementations of the Wi-Fi WPA2 security.

Official details of the vulnerability are tracked via a number of Common Vulnerabilities and Exposures, or CVEs. CVEs can be looked up at https://cve.mitre.org.

Vulnerabilities

The CVEs associated with the *KRACK* attack can be grouped 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 device. If the vulnerability exists, it will exist in code that implements the security **supplicant** as defined in the 802.11 specification.

These CVEs pose a serious risk which can result in decryption of network traffic and replay of previously sent frames or forging of new frames.

Linux-Based Solutions

For devices using Linux as the primary operating system, an open source package called *wpa_supplicant* is usually used to implement the 802.11 supplicant functionality.

Customers who obtain *wpa_supplicant* directly from the open source project can check for the latest updates that address these issues. For customers receiving a version of *wpa_supplicant* directly from Cypress, please see the *Release Information* section below.

WICED-Based Solutions

In WICED Studio, the **supplicant** functionality is implemented in the firmware that runs on the specific Cypress Wi-Fi chipsets.

The following table lists which WICED chipsets have vulnerable firmware implementations for this group of CVEs:

Chipset	Vulnerable to Group 1 CVEs
43362	No
43903	No
43907	No
43909	No
54907	No

43340	No
43364	Yes
43438	Yes
4343W	Yes

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.

As with the Group 1 CVEs, a change to the security **supplicant** is needed to address any vulnerable implementations.

Linux-Based Solutions

All versions of *wpa_supplicant* prior to the KRACK attack are vulnerable.

Customers who obtain *wpa_supplicant* directly from the open source project can check for the latest updates that address these issues. For customers receiving a version of *wpa_supplicant* directly from Cypress, please see the *Release Information* section below.

WICED-Based Solutions

All versions of firmware used in WICED releases contain the vulnerabilities from Group 2 in the **supplicant** function.

Please see the *Release Information* section below.

GROUP 3:

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

CVE-2017-13082 describes a vulnerability in Access Points (APs) that implement the FT reassociation requests associated with 802.11r. The other CVEs describe vulnerabilities in station devices that implement the *PeerKey* handshake and other specific wireless network management exchanges.

Cypress chipsets and current software releases are not affected by these CVEs.

Release Information

Linux Releases and Automotive Segments

The upcoming Linux Q4 release, scheduled for October 28, 2017, will include an updated version of *wpa_supplicant* that will address all vulnerabilities in Group 1 and Group 2.

Additionally, Cypress will provide an updated version of *wpa_supplicant* with features specific for the automotive segment. This will be provided to customers no later than October 23, 2017.

WICED Studio Releases

The upcoming WICED Studio 6.0 release, scheduled for October 28, 2017, will address the CVEs in Group 1 and Group 2.

Additionally, Cypress is currently patching and testing updates to previous WICED Studio packages to address the CVEs in groups 1 and 2 above. Updates to the following WICED Studio releases will be posted to the http://community.cypress.com the week of October 31, 2017:

- WICED Studio 4.1.3
- WICED Studio 5.2

For updates to other WICED versions, please reach out to your Cypress sales representative.