KRACK vulnerability and Digi Embedded for Android

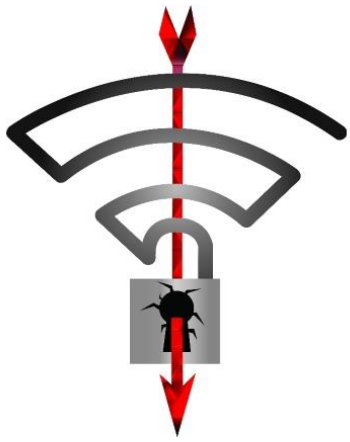
November 2017

Introduction

This document provides instructions for updating Digi Embedded for Android to integrate the fixes for the KRACK vulnerability. This document applies to Android 4.4 and Android 5.1 running on Digi's ConnectCore 6 SoM family.

KRACK

On October 16th, 2017, a public vulnerability was released that impacts the Wi-Fi "over the air" encryption protocol known as WPA/WPA2. The attack is called "KRACK" for "Key Reinstallation Attacks". These vulnerabilities allow an attacker to intercept and in some special cases inject network traffic between a Wi-Fi Client and a Wi-Fi Access Point. This attack can only be performed if the attacker is within radio intercept distance of a Client and Access Point. It is noted that with the discovered vulnerabilities, BOTH the Client and the Access Point must be fixed to fully protect the network traffic. The impact of this vulnerability is only against the transport layer. Other encryption, such as TLS 1.2 that is done at other layers, is NOT impacted and can be considered safe. However, with a corrupted transport layer, it may be possible to conduct other attacks like man in the middle (MitM) attacks by tricking end users.



Digi Wi-Fi products using Digi Embedded for Android **are affected** by the KRACK vulnerability **when using Client Modes**. Note that **Access Point Modes are not affected** with the default wpa_supplicant/hostap configuration provided because Fast Transition is disabled.

Installation instructions

Patch the source code

NOTE: If you build Android from scratch and want to include the patches in your builds, follow these instructions. If not, proceed to the next section.

To fix the KRACK vulnerability in your DEA system image, you must apply a specific set of patches to the **wpa_supplicant/hostapd** package found in **external/wpa_supplicant_8** in the Android source code. These patches have been condensed into a single one for each Android version to simplify the patching process. Each patch is prefixed with the Android version it applies to.

To apply the patch, move it to the **external/wpa_supplicant_8** directory and run the following command via a command line:

```
patch -p1 < DEA-<version>-PATCH-fix-WPA2-key-replay-security-bug.patch
```

If no changes have been made to that directory, the patch should apply cleanly. In other cases, you may need to hand-pick the changes from the patch file into the source code.

Once you have patched the package, rebuild the system image.

Update your current images

You can update your hostapd and wpa_supplicant binaries in your current Android system by replacing them with their respective patched versions.

1. **Remount the system partition in read-write mode** via the Android command line. To see which device path the system partition is mounted from, read the **/fstab.mmcblk*X*.ccimx6sbc** file where *X* is:
   - **0** if your Android system is stored in the MMC
   - **1** if your Android system is stored on an SD card

   For example, on DEA 5.1 booted from MMC, the device path is **/dev/block/mmcblk0p3**.
2. Run the following command:

   ```
   mount –o rw,remount <device_path> /system
   ```

3. Transfer the patched binaries to your target in the **/system/bin** directory, either via **adb push** from your development machine, **scp** over the network, or any other transfer method.
4. Once the binaries have been transferred, change their permissions:

   ```
   chmod 755 <filename>; chown root:shell <filename>; sync
   ```

Your target is now patched for the KRACK vulnerability.

Additional information

Visit Digi Security Center for the latest news about security on Digi's products or contact tech.support@digi.com if you have further questions.

You can also find more information at KRACK vulnerability.