Title: **Wi-Fi Protected Access Key Reinstallation Attack (KRACK)**
Advisory ID: CARESTREAM-XRS-2017-01
Issue Date: 11/01/2017
Last Revision Date: 12/28/2017
CVE(s):

CVE-2017-13077
CVE-2017-13078
CVE-2017-13079
CVE-2017-13080
CVE-2017-13081
CVE-2017-13082
CVE-2017-13084
CVE-2017-13086
CVE-2017-13087
CVE-2017-13088

What is the Key Reinstallation Attack?

The Key Reinstallation Attack (KRACK) refers to an attack method that takes advantage of several flaws in the Wi-Fi Protected Access II (WPA2) security protocol. WPA2 is used as the default wireless security protocol in the majority of commercial and consumer Wi-Fi enabled devices. If successfully exploited attackers can eavesdrop on communications and potentially alter message content. Attackers must be within Wi-Fi range to execute an attack.

For additional information on *the vulnerabilities please visit*:
https://www.kb.cert.org/vuls/id/228519/

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080

Are Carestream Products Vulnerable?

Carestream Imaging Systems' products use WPA2 secured Wi-Fi in two distinct ways;

1) Communication with DRX Wireless Detectors on an isolated private network with a dedicated access point (DRX Private Network). The potential risk associated with KRACK specific to the DRX Private Network communication is low. Communication on the DRX Private Network includes no PHI (Protected Health Information) data by design.

   Affected Products:

   DRX-Evolution with DRX-1 or DRX-Plus Wireless Detectors
   DRX-Ascend with DRX-1 or DRX-Plus Wireless Detectors
   DRX-Innovation with DRX-Plus Wireless Detectors
   DRX-Excel with DRX-Plus Detectors
   DRX-1 System
   DRX-Revolution
   DRX-Mobile Retrofit (all models)
   DRX-Transportable (all models)
   Image Suite with DRX-1 or DRX-Plus Detectors

   Carestream is currently working on patches for DRX-1 and DRX-Plus Detectors and will make these available in the next planned product release. Carestream is also working with our Access Point vendors to secure firmware updates with expected availability of Q1 2018.

   How can I mitigate the risk to my equipment / data?

Carestream DRX room solutions support the use of a wired network connection for communication with DRX Detectors via an optional tethered interface. Customers may choose to operate in tethered only mode.

Attackers must be within Wi-Fi range of the network they attempt to attack. To minimize the coverage of the DRX Private Network, customers may elect to reduce the access point power level to the lowest level required to achieve the required system performance.

2) Communication between Carestream product's and other end points on customer networks. This communication includes PHI (Protected Health Information) by design. These products run various versions of the Microsoft Windows Embedded Operating system.

Affected products:

DRX-Revolution
DRX-Mobile Retrofit
DRX-Transportable (all models)
Touch Prime
Touch Prime XE

Patch Availability

Product	Version(s)	Patch Available
DRX-Revolution	5.7E MR2	Yes
DRX-Mobile Retrofit	5.7E MR2	Yes
DRX-Transportable (all models)	5.7E MR2	Yes
Touch Prime	1.0 P6	Yes
Touch Prime XE	1.0 P6	Yes

For customers with products running DirectView software versions prior to 5.7 no Microsoft patches are available for your products. Please contact your Carestream Sales or Service Sales representation for upgrade options.

How can I mitigate the risk to my equipment / data?

Carestream highly recommends use of a Virtual Private Network (VPN) to encrypt all traffic on your network.

Please contact your Carestream sales, service sales, or field service representative to coordinate patch installation or if you have additional questions.