Canon

Canon Medical Systems USA, Inc.

Key Reinstallation Attacks, AKA Krack

Vulnerability Note VU#228519 http://www.kb.cert.org/vuls/id/228519

Overview:

Wi-Fi Protected Access (WPA, more commonly WPA2) handshake traffic can be manipulated to induce nonce and session key reuse, resulting in key reinstallation by a wireless access point (AP) or client. An attacker within range of an affected AP and client may leverage these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocols being used. Attacks may include arbitrary packet decryption and injection, TCP connection hijacking, HTTP content injection, or the replay of unicast and group-addressed frames. These vulnerabilities are referred to as Key Reinstallation Attacks or "KRACK" attacks. (REF: http://www.kb.cert.org/vuls/id/228519)

This type of attack is quite complicated and difficult to implement at the facility. The difficulty is due to the need for the attacker to be within range of the Wi-Fi device during the WPA negotiation between devices which is only performed during initial handshaking. Information security risk is not exacerbated by this vulnerability.

Possible Affected Canon Products (investigating):

XR Wireless Flat Panel Detector (FPD)

• DIGITAL RADIOGRAPHY SYSTEM DRAD-3000E

TFP-4336W: Optional Configuration, Wi-Fi Access Point

Ultrasound

• Ultrasound Aplio™ 300/500 (UIWL-A500A): Optional Configuration

• Ultrasound Xario™ 100/200 (UIWL-X200A): Optional Configuration

• Ultrasound Aplio™ i700/800/900 (UIWL-A500A): Optional Configuration

• Ultrasound Aplio™ i700/800/900 (UITB-AI900A): Optional Configuration

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life

Unaffected Products

- XR Wireless foot-switch (Bluetooth)
- MR Wireless peripheral devices (Proprietary communication protocol)
- All Computed Tomography (CT) products (AKA TSX, Aquilion, Prime, Vision, Genesis)
- All X-Ray Angiographic / Vascular Imaging (AKA Infinix, DFP-8000)
- All Magnetic Resonance Imaging (MRI) (AKA Titan, Galan, Elan, GP)
- All Ultrasound systems that implement a physical network connection
- All X-Ray systems that have wired Direct Radiography (DR) panels
  2441 Michelle Drive, Tustin, CA 92780 / 800.421.1968 / http://us.medical.canon
- Harmony (AKA HDR-08A, Kalare, Ultimax)
- EPS+ (AKA Kalare, Ultimax)

Resolution

Canon Medical is actively investigating the applicability for the affected systems.

Notes:

Continue to check this advisory for updated information. Please email CanonUSASecurity@us.medical.canon with any specific questions or issues.

Vulnerability Information

- CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake
- CVE-2017-13078: reinstallation of the group key in the Four-way handshake
- CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake
- CVE-2017-13080: reinstallation of the group key in the Group Key handshake
- CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake
- CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key 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
- CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

Advisory Change Log

This is the initial release of this advisory.

CANON MEDICAL SYSTEMS USA, INC.
2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life