Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
-
Phone number
+49 451 882-6166

E-mail
hannes.molsen@draeger.com
scott.bristol@draeger.com
fabian.busch@draeger.com

Vulnerability and Incident Reporting
product-security@draeger.com

Dräger Product Security Advisory 201704
KRACK Attacks WPA2 Vulnerabilities

To whom it may concern,

On October 16, 2017, a global coordinated disclosure revealed a vulnerability in the widely used WPA2 encryption standard for wireless networks. It was discovered by researchers Mathy Vanhoef and Frank Piessens of KU Leuven in Belgium and called KRACK Attacks[1], short for Key Reinstallation Attacks. This attack works against the encryption mechanism used in the WPA2 protocol to transmit data securely. As this is a flaw in the Wi-Fi standard description of the so called four-way handshake, it is highly likely that most implementations of the protocol are affected by this.

To connect to Wi-Fi Networks, Dräger's devices are equipped with off-the-shelf Wi-Fi Modules and Chipsets developed and maintained by the respective manufacturers. The manufacturers were contacted by Dräger immediately asking whether their implementations are affected by the vulnerability, and if, when a fix will be available. At the time of writing these manufacturers did not yet provide answers.

Nevertheless until proven wrong, we assume the following devices are affected by the KRACK vulnerabilities:

[1] https://www.krackattacks.com/

Product	Status
Infinity® M300 (Hardware Revision <0.4)	Used Chipset: NXP Semiconductors BGW211
Infinity® M300 (Hardware Revision ≥0.4)	Used Chipset: Redpine Signals RS9113
Infinity® M540 (older Hardware Revisions)	Used Chipset: NXP Semiconductors BGW211
Infinity® M540 (latest Hardware Revisions)	Used Chipset: Redpine Signals RS9113
Infinity® Delta Series (all Hardware Revisions)	Used Chipset: Ambicom Wireless Card
Vista 120 S	Used Chipset: Redpine Signals RS9113

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Prof. Dr. Nikolaus Schweickart
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

Impact

The KRACK attacks vulnerabilities can be carried out by an attacker in proximity, i.e., Wi-Fi-range of the attacked device. Furthermore, while the vulnerability is already published, no ready-to-use exploit code or tools have been made available to the public so far, therefore a highly skilled attacker is needed to carry out an attack. Nevertheless, due to the details given in the published paper[2], we expect such tools to be published in the coming weeks.

By carrying out KRACK, an attacker is first of all able to decrypt and read data transmitted over the air. The packets in the Infinity Network can – but must not – contain Personal Health Information (PHI), which is linked to an individual if the patient name is configured on the Infinity® M300, Infinity® M540 or Infinity® Delta Series devices. Dräger recommends to the responsible organization to consider to refrain from using the patient name field on the affected devices.

If the Wi-Fi network access point is configured to use WPA-TKIP or GCMP an attacker is able to replay and forge network packets. We suggest to use the AES-CCMP encryption protocol. While packets can still be deciphered in AES-CCMP using KRACK, only TCP connections can be intercepted combining the KRACK attack with a TCP network sequence prediction attack[3]. For the Infinity® M300, Infinity® M540, and Infinity® Delta Series monitors in the Infinity® network, clinical data is transmitted using UDP packets, this configuration seems to be unaffected by the packet forgery and replay attack.

We are actively monitoring the situation, waiting for the responses of the chipset vendors and evaluating possible further steps.

[2] http://papers.mathyvanhoef.com/ccs2017.pdf
[3] https://en.wikipedia.org/wiki/TCP_sequence_prediction_attack

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Prof. Dr. Nikolaus Schweickart
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

Conclusion and Proposed Mitigations

Due to the high sophistication and close proximity needed to carry out an attack, and the low value of the information an attacker would be able to decrypt, we estimate the risk of a successful attack against the possibly affected devices as improbable. Nevertheless, to further reduce the risk of PHI to be leaked, we suggest to refrain from using the patient name fields. To reduce the risk of forged messages introduced on the WiFi channel, we suggest to configure the network to use AES-CCMP encryption.

Further Information

- The Wi-Fi network's keys are not revealed by the attack. The network passwords are used to authenticate devices against the network. The KRACK attacks work on the subsequent process: the encryption of the data packets sent over the air. It is not necessary to change the network passwords at this point.
- With AES-CCMP there is no increased risk to patient safety, as packets can't be forged.

If you have any further questions related to the impact of the KRACK attacks vulnerability on Dräger devices, please contact your designated regional marketing manager. For reporting incidents and potential vulnerabilities in our devices, please refer to https://static.draeger.com/security to contact the Product Security team directly.

Best regards,

Dräger Product Security

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Prof. Dr. Nikolaus Schweickart
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner