PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

24 September 2018
S1: 300389504 /pbsa56

# Security Advisory for Phoenix Contact WLAN enabled devices utilizing WPA2 encryption [Update 2018-09-24]

## Synopsis

Multiple security issues and vulnerabilities within the WPA2 standard have been identified and publicized by Mr. Mathy Vanhoef and KU Leuven (https://www.krackattacks.com). These vulnerabilities may allow the reinstallation of a pairwise transient key, a group key, or an integrity key on either a wireless client or a wireless access point (AP). In consequence an attacker could establish a man-in-the-middle position between AP and client facilitating packet decryption and injection.

## Affected devices

Phoenix Contact is currently working on identifying affected devices.
Phoenix Contact embedded devices used in AP mode are not affected. To current knowledge due to the firmware properties embedded devices used in client or repeater mode are only affected by 3 out of 10 published CVEs assigned to this vulnerability (CVE-2017-13077, CVE-2017-13078, CVE-2017-13080).
Phoenix Contact devices running Microsoft Windows are affected.

## Impact

Phoenix Contact embedded devices running in AP mode are not affected by these vulnerabilities. If devices are used in client or repeater mode, an attacker could in theory decrypt any packet sent by the client. Devices of the FL WLAN 110x, 210x, and 510x product families are only affected to a very limited extent. With these devices, only data packets sent within three seconds after key renewal could possibly be decrypted by a successful attacker. In general, if TCP SYN packets are decrypted, this could be used to hijack TCP connections and inject malicious traffic into unencrypted protocols.
However, to perform the attack, the attacker must be significantly closer to the WLAN client than the access point. In industrial or indoor applications, the attacker would have to be inside the plant. A successful external attack therefore seems to be very difficult.



...

Furthermore, the WPA2 password cannot be compromised using a KRACK attack. It is not possible for the attacker to gain full access to the network. However, please note that if WPA-TKIP is used instead of AES-CCMP, the impact of this vulnerability is more severe, because an attacker might be able not only to decrypt packets, but also to forge and inject packets directly into the WLAN.

Solution

Phoenix Contact is currently in the process of reviewing which of our devices may be affected by this vulnerability and will update the advisory including information about patches provided.
For Phoenix Contact devices running Microsoft Windows, we recommend to apply the security update provided by Microsoft.
If you are using WPA-TKIP in your WLAN, we recommend switching to AES-CCMP.

This advisory will be updated as further details become available.

Update 2017-11-09

Below you may find an overview of affected product names and article numbers. For products of which several variants are available, the product name was grouped and shortened (identifiable by “*”). The list of article numbers contains all product variants.

| Articles | Article numbers | Product state |
|---|---|---|
| BL2 BPC * | 2404777, 2404845 | current |
| BL2 PPC * | 2404844, 2404846 | current |
| FL COMSERVER WLAN 232/422/485 | 2313559 | discontinued |
| FL WLAN 110x | 2702538, 2702534 | current |
| FL WLAN 210x | 2702535, 2702540 | current |
| FL WLAN 510x | 2700718, 2701093, 2701850 | current |
| FL WLAN 230 AP 802-11* | 2884444, 2700452 | discontinued |
| FL WLAN 24 AP 802-11* | 2700448, 2884075 | discontinued |
| FL WLAN 24 DAP 802-11* | 2884279, 2700451 | discontinued |
| FL WLAN 24 EC 802-11* | 2884130, 2700449 | discontinued |
| FL WLAN EPA* | 2692791, 2700488, 2701169 | discontinued |
| FL WLAN SPA | 2884761 | discontinued |
| ITC 8113* | 2403738, 2403485, 2402911, 2403267, 2402979, 2402957 - 2402964 | current |
| RAD-80211-XD* | 2885728, 2900046, 2900047, 2990011 | discontinued |
| RAD-WHG/WLAN-XD | 2900178 | current |
| TPC 6013* | 2913784, 2700740, 2700611, 2701316 | discontinued |
| VMT 30xx | 2913852, 2701003, 2700969, 2913959, 2700878 | discontinued |
| VMT 50xx | 2887580, 2887593, 2887593, 2913810 | discontinued |
| VMT 70xx | 2400158 - 2400161 | current |

...

Update 2018-09-24

For the following products a firmware update addressing the issues is available for download on the Download tab of the corresponding product page on our website:

| Articles | Firmware version | Released |
|---|---|---|
| FL EPA 2,<br>FL EPA 2 RSMA | FW 1.53 or higher | 06/2018 |
| FL WLAN 5100,<br>FL WLAN 5101,<br>FL WLAN 5102,<br>FL WLAN 5110,<br>FL WLAN 5111 | FW 3.06 or higher | 06/2018 |
| FL WLAN 1100,<br>FL WLAN 1101,<br>FL WLAN 2100,<br>FL WLAN 2101 | FW 2.21 or higher | 06/2018 |