

WirelessHART® Unaffected by Recent WPA2 Vulnerabilities

1.0 Key points

- Multiple vulnerabilities have been discovered that affect WPA2, which is used to secure Wi-Fi connections
- *WirelessHART* and Wi-Fi are completely different technologies
- *WirelessHART* is unaffected by these vulnerabilities

2.0 Background

Recently, two Belgian researchers discovered multiple vulnerabilities which affect the Wi-Fi Protected Access II (WPA2) protocol. WPA2 is a network security technology used to secure Wi-Fi internet connections. WPA2 replaces the older WPA technology which, in turn, replaced WEP technology for securing Wi-Fi connections.

The vulnerabilities recently disclosed by the Belgian researchers are getting significant press coverage and the suite of vulnerabilities has been named “KRACK”. The KRACK name is derived from Key Reinstallation Attack, and the researchers are claiming that almost every Wi-Fi device is vulnerable to some variant of their attacks.

These vulnerabilities abuse design or implementation flaws in cryptographic protocols to reinstall an already-in-use or predictable key. Depending on the specific vulnerabilities that are exploited, an attacker can decrypt network information allowing the attacker to read contents of messages, inject malicious content, pose as a legitimate access point, or perform other nefarious activities.

3.0 *WirelessHART* is not Wi-Fi

WirelessHART can sometimes be confused with Wi-Fi since both are wireless technologies. While they share a few similarities, they are very different technologies.



Although both *WirelessHART* and Wi-Fi both operate at 2.4 GHz (Wi-Fi can also use 5GHz), there are a lot of differences. To start with, *WirelessHART* operates with an 802.15.4 radio while Wi-Fi uses an 802.11 radio. This means that Wi-Fi devices and *WirelessHART* devices communicate in completely different ways. As mentioned above, Wi-Fi uses a technology called WPA2 to secure the connections between devices while *WirelessHART* uses a join key (delivered out of band) to secure the initial connection between devices. *WirelessHART* is a low-power wireless protocol used to transmit relatively small amounts of data while Wi-Fi can be used to transfer large amounts of data, including video streams and large file transfers. Another major area where *WirelessHART* differs from Wi-Fi is the fact that the security mechanisms cannot be disabled in

WirelessHART. In Wi-Fi, although not advised, a user could disable security features and operate without any encryption or authentication whatsoever.

Further information on *WirelessHART* security can be found here:

[Emerson Wireless Security](#)

4.0 Guidance

It is important to apply patches as vendors issue them. These patches will prevent key reuse and will be backwards-compatible, meaning patched clients can communicate with unpatched access points and vice-versa but both the client and AP must be patched to prevent against the attacks.

Although Emerson™ *WirelessHART* Gateways are not affected by this vulnerability, the Cisco® 1552WU is an access point which utilizes both *WirelessHART* and Wi-Fi. If you or your customer are using a Cisco 1552WU, it is important to advise them to visit the [Cisco website](#) for Cisco's notification and software update regarding this vulnerability as soon as possible.

Using other encrypted protocols, such as Hyper Text Transfer Protocol Secure (HTTPS), can offer another layer of protection. HTTPS was designed to work over an untrusted channel with no encryption and should be used when possible. Also, using a Virtual Private Network (VPN) can offer additional protection against these attacks.

Finally, using a wired connection for sensitive traffic eliminates these concerns.

The researchers have provided a good writeup. For additional information, their site can be found here:

[Krackattacks.com](#)

Global Headquarters

Emerson Automation Solutions

6021 Innovation Blvd.

Shakopee, MN 55379, USA

+1 800 999 9307 or +1 952 906 8888

+1 952 949 7001

RFQ.RMD-RCC@Emerson.com

North America Regional Office

Emerson Automation Solutions

8200 Market Blvd.

Chanhassen, MN 55317, USA

+1 800 999 9307 or +1 952 906 8888

+1 952 949 7001

RMT-NA.RCCRFQ@Emerson.com

Latin America Regional Office

Emerson Automation Solutions

1300 Concord Terrace, Suite 400

Sunrise, FL 33323, USA

+1 954 846 5030

+1 954 846 5121

RFQ.RMD-RCC@Emerson.com

Europe Regional Office

Emerson Automation Solutions Europe GmbH

Neuhofstrasse 19a P.O. Box 1046

CH 6340 Baar

Switzerland

+41 (0) 41 768 6111

+41 (0) 41 768 6300

RFQ.RMD-RCC@Emerson.com

Asia Pacific Regional Office

Emerson Automation Solutions Asia Pacific Pte Ltd

1 Pandan Crescent

Singapore 128461

+65 6777 8211

+65 6777 0947

Enquiries@AP.Emerson.com

Middle East and Africa Regional Office

Emerson Automation Solutions

Emerson FZE P.O. Box 17033


Jebel Ali Free Zone - South 2

Dubai, United Arab Emirates

+971 4 8118100


+971 4 8865465


RFQ.RMTMEA@Emerson.com

 [Linkedin.com/company/Emerson-Automation-Solutions](https://www.linkedin.com/company/Emerson-Automation-Solutions)

 [Twitter.com/Rosemount_News](https://twitter.com/Rosemount_News)

 [Facebook.com/Rosemount](https://www.facebook.com/Rosemount)

 [Youtube.com/user/RosemountMeasurement](https://www.youtube.com/user/RosemountMeasurement)

 [Google.com/+RosemountMeasurement](https://www.google.com/+RosemountMeasurement)

Standard Terms and Conditions of Sale can be found on the [Terms and Conditions of Sale page](#).

The Emerson logo is a trademark and service mark of Emerson Electric Co.

Rosemount and Rosemount logotype are trademarks of Emerson.

WirelessHART is a registered trademark of the FieldComm Group.

Cisco is a registered trademark of Cisco Systems, Inc.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

All other marks are the property of their respective owners.

© 2017 Emerson. All rights reserved.



