Technical Bulletin CS-17-07

KRACK – WPA2 Security Vulnerability

This technical bulletin explains the impact of the KRACK security vulnerability to the Spectralink Wi-Fi product lines

System Affected

Spectralink PIVOT (87-Series), 84-Series handsets, 80-Series handsets and QNC

Description

The Key Reinstallation AttACK (KRACK) vulnerability exploits a flaw in the Wi-Fi Protected Access II (WPA2) Wi-Fi encryption protocol.This vulnerability affects many different devices running Android, iOS, Linux, and Windows operating systems. And the vulnerability applies to both Personal (PSK) and Enterprise (802.1X) modes.

The vulnerability can provide attackers with the ability to eavesdrop traffic to and from the attacked vulnerable device. Potentially the attacker could inject malicious traffic towards the attacked device or towards the far-end device. It does not directly give the attacker the wireless PSK key however.

KRACK exploits the four-way handshake executed when a client joins a WPA2 wireless network, and tricks devices to reinstall already in-use keys that can result in undermining the encryption. Variations of the attack exist and these affect different vendor's equipment with differing degrees of severity, so it is important to patch all Wi-Fi devices in a timely manner.

We highly recommend that customer ensure their WLAN infrastructure is updated as soon as patches become available from their respective WLAN vendors. Any customer using WPA2-PSK should ensure they are using AES rather than TKIP. Packet injection is only possible in TKIP, but is not possible when using AES. Additionally, patching the WLAN infrastructure eliminates a more common attack vector. Anyone attempting to attack a phone would only be able to decrypt traffic from the phone to the AP, one device at a time. They would not be able to decrypt any traffic from the AP to the phone.

PIVOT handset uses a different version of the WPA Android supplicant which is not susceptible to the zero key insert exploit. However, we are vulnerable to some of the other exploits. Google has provided a security patch to Spectralink to allow us to patch the Android operating system

to address the reported vulnerability. We have posted software release 2.5.1.20865 to the Spectralink Support Portal as of December 8, 2017.

A software release will also be made available for Spectralink 84-Series handsets with the necessary code changes to remediate the vulnerability. Software release 5.4.4D.x167 was posted to the Spectralink Support Portal on November 6, 2017.

The SpectralinK QNC (Quick Network Connector) tool is susceptible to this exploit only when using the Wi-Fi provisioning method with handsets. This tool uses a Linux operating system which we will patch by the end of 2017. The impact to this device is much more limited due to the reduced operating range of the radio.

The Spectralink 80-Series handset models are affected but will not be receiving any software updates to correct for this issue. These handsets have reached their end-of-life state and are no longer being supported with software updates.

Document Status Sheet

Document Control Number: CS-17-07

Document Title: KRACK – WPA2 Security Vulnerability

Revision History: I01 – Released *October 17, 2017*
I02 – Released
I03 – Released

Date: *10/17/2017*

Status: ☐Draft ☒Issued ☐Closed

Distribution Status: ☐Author Only ☐Internal ☐Partner ☒Public

Copyright Notice

Notice

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at http://support.spectralink.com.

Contact Information

US Location
+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location
+44 (0) 20 3284 1536

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com