IMPORTANT Security Vulnerability Notice: Response to Key Reinstallation Attacks (KRACK)
Products Affected: WavePro WP201-100
Date: October 19, 2017

Summary

On October 16, 2017 a research team announced vulnerabilities in the Wi-Fi Protected Access II (WPA2) protocol used in all Wi-Fi networks. These vulnerabilities are specific to this commonly used protocol, therefore, **all vendors of Wi-Fi products are affected**. **There is no evidence that these vulnerabilities have been exploited for malicious intent**. FreeWave Technologies is determining the impact of this vulnerability on its WavePro WP201-100 Wi-Fi Access Point and will release a software patch shortly. In the meantime, we recommend continuing to use the WavePro product utilizing WPA2 with “Fast Roaming” disabled.

Research Overview

On October 16, 2017 a researcher at KU Leuven announced the discovery of vulnerabilities in the Wi-Fi Protected Access II (WPA2) protocol. The research is titled “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2” and is commonly known as “KRACK”. The vulnerabilities identified are specific to the WPA2 protocol and provide evidence that an attacker could intercept information being sent over the network. WPA2 is the most commonly used security protocol for protecting Wi-Fi networks and, even unpatched, is still considered the least vulnerable.

Key Points

- These vulnerabilities apply to the Wi-Fi protocol, therefore, all Wi-Fi vendors are impacted.
- There is no evidence that these vulnerabilities have been exploited for malicious intent.
- Key considerations that impact the vulnerability of a network:
  - The attacker must be in the physical proximity of the network.
  - The attack is technically sophisticated. The attacker must first perform the key reinstallation attack and then decrypt the information intercepted.
- Industry experts recommend the continued use of WPA2. Even with these identified vulnerabilities and unpatched devices, WPA2 is still the best security protocol for Wi-Fi networks.

Impact

FreeWave engineering is currently evaluating the WP201-100 product for the impact of these vulnerabilities on the different operation modes of the product. At this time, we believe:

- The standard "Access Point" operation mode is not vulnerable.
- All other operation modes including mesh and point-to-point are likely vulnerable.
- Operation using "Fast Roaming" (based on 802.11r) is vulnerable. This feature is disabled by default.

Software Patch

A software update for the WavePro WP201-100 will be available shortly. We will send out a notice to alert all existing customers of the need to update the WP201 software.

Most manufacturers of Wi-Fi products are implementing software patches to eliminate the risk and are releasing updates in the coming weeks. During this transition period, patched and unpatched devices are cross-compatible.

Once available, the new software and update instructions will be located on FreeWave's Support Site: http://support.freewave.com/ in the "WavePro WP201 Industrial Wi-Fi" folder.

Additional Reading

Wi-Fi industry groups, consortiums and thought leaders are providing much of the consolidated information about KRACK attacks. Here are a selection of Wi-Fi industry notices for further information:

- KRACK Website: https://www.krackattacks.com/
- Full Research paper: https://papers.mathyvanhoef.com/ccs2017.pdf
- Cert/CC Vulnerability Notice: https://www.kb.cert.org/vuls/id/228519

Contact Us

If you have further questions beyond the information provided above, please contact FreeWave customer support at 1-866-923-6168 or support@freewave.com.