KR00K WI-FI SECURITY VULNERABILITY

A White Paper

May 2020

unitech

because we care

Preface

Unitech are committed to ensure our customers are safe in choosing, and using, our products and solutions. Therefore, we have closely monitored a *potential threat* which may compromise this pledge, by offering some guidance and additional information in a timely manner.

Unitech wish to name one of the threats called “Kr00k” that has been in use since summer 2019 that has caused companies to be exploited by unlawful hacks.

1. What is “Kr00k”

Kr00k is a security vulnerability that allows some WPA2 encrypted Wi-Fi traffic to be decrypted unbeknownst to the user/s. The vulnerability was originally discovered by security company ESET in 2019 and was originally named: CVE-2019-15126 on August 17th, 2019.

The Kr00k susceptibility affects all Wi-Fi-capable devices, including access points that use Wi-Fi chips made by Broadcom or Cypress, this allows unauthorized decryption of some WPA2 encrypted traffic. Consequently, there are other brands and devices that are at risk from Kr00k and we recommend you learn more via the link here: 2. Additional Information

Because we care, Unitech have carefully reviewed, with our chipset vendors, in respect to which of our Unitech devices could be at risk. We are happy to confirm that many of our devices including our 3 flagship enterprise devices: PA760, EA510 and EA5100+, our handheld terminals: HT380 and HT510 and even our latest’s tablets: TB162 (Windows 10 IoT) and TB85 (Android 8) are safe to use without the threat or worry of the Kr00k vulnerability. However, we would like to inform you that two of our older devices, the PA692 and HT682 series, are affected.

For these two devices, we are working closely and quickly on a solution with our chip vendors to fix this issue. We will announce, in due course, a schedule release of a fix once our chip partners have released the schedule to us. In the meantime, we would like to advise customers to use TLS data encryption instead of WPA2 when it is possible. Because TLS tunneled data is not at risk by the kr00k vulnerability.

If you need further information on Kr00k then please do not hesitate to contact Unitech.

2. Additional Information:

Information regarding Kr00k from ESET:

https://www.eset.com/int/kr00k/

3. About Unitech:

Unitech was founded in 1979 in Taipei, Taiwan. As a global provider of automatic identification and data capture technologies, Unitech manufactures a wide range of rugged mobile computers, RFID readers and fixed mount terminals. Unitech products bring value to customers throughout the world in various industries, i.e. transportation, logistics, retail, banking, warehouse and manufacturing. Our goal is to develop solutions that help our customers achieve higher productivity and more efficient operations.

Unitech Europe is in Tilburg, the Netherlands, since 1999. From this location the Unitech products are distributed throughout Europe, Africa and the Middle East. Beside distribution the Tilburg location of Unitech also provides extensive service in the field of sales, marketing and technical support. By this local service Unitech Europe is capable to react quickly and properly to customers' and potential partners' *questions and needs.*

Unitech Europe
Kapitein Hatterasstraat 19
5015 BB Tilburg
The Netherlands
+31 (0) 13 460 9292
+31 (0) 13 460 9293
http://eu.ute.com

If you have any question or request further information, then please do not hesitate to let us know. You can reach us via http://eu.ute.com contact tab.

The content of this document is based on Unitech's knowledge built up in the years of experience the company has in the mobility industry. Unitech accepts no responsibility for any liability arising from use of this document of its contents. Nothing in this note constitutes or should be taken to constitute investment advice.