INTERNET SERVICE PROVIDERS
ASSOCIATION OF NEW ZEALAND

ISPANZ INFORMATION PAPER

WPA2 Security Vulnerability

Introduction

It has recently (October 2017) been identified that the WPA2 WiFi security standard contains a significant vulnerability. The original research paper documenting the issue is here:

https://papers.mathyvanhoef.com/ccs2017.pdf

A discussion of the key points is here:

https://techcrunch.com/2017/10/16/wpa2-shown-to-be-vulnerable-to-key-reinstallation-attacks/?utm_medium=TCnewsletter

What is This Security Vulnerability?

The vulnerability applies to the WPA2 security standard. As it is a flaw in the standard itself, it is likely to apply to all Wifi devices implementing WPA2. A database of vendors with potential vulnerabilities is here:

https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4

When a new device connects to a Wi-Fi signal, WPA2 uses a four-way handshake where the Wi-Fi network authenticates itself to the new device and generates a one-time encryption key for the Wi-Fi session. An attacker within the Wi-Fi's range could use key reinstallation attacks (KRACKs) to trick the handshake into reinstalling a used encryption key. This then allows the attacker into the network, and able to access personal data or inject ransomware or malware.

How Could it Affect Customers?

Customers could have their equipment and networks compromised.in a number of ways, including losing their private data, being subjected to a ransomware attack or have their equipment rendered inoperable.

What Advice Would Help Customers?

- Equipment vendors have been developing patches to their WPA2 software, so the first advice to give to customers is to ensure that they download and install the latest updates for all their WPA2 enabled devices. They should remember that these include not just desktops and laptops, but also wireless routers, phones, tablets, Kindles, printers and entertainment devices such as Amazon Echo, as well as WiFi enabled devices in their cars and on their boats.
- Using a VPN improves WiFi security. You may wish to offer or recommend VPN solutions to your customers.
- Customers should **not** switch to the older WEP standard as a temporary fix. Its security is much worse than WPA2.