TELECOMS - TAIWAN

NCC warns of WiFi security breach

November 01 2017 | Contributed by Shay & Partners

AUTHOR

Arthur Shay

On October 18 2017, further to the US Computer Emergency Readiness Team issuing a warning in response to the key reinstallation attack that takes advantage of vulnerabilities in WiFi security to let attackers eavesdrop on traffic between computers and wireless access points, the National Communications Commission (NCC) issued a warning regarding the breach and urged network operators and equipment providers to fix this unprecedented flaw in WiFi protection that has left almost all home routers at risk of being hacked. The NCC believes the risk to be imminent.

In Taiwan, telecommunications subscribers generally use free WiFi internet access (which is almost ubiquitous) as an alternative to mobile 4G internet access. For example, Chunghwa Telecom, the largest telecommunications carrier in Taiwan, has over 4.3 million broadband subscribers, which consist of 3.53 million fibre-optic subscribers and over 800,000 asymmetric digital subscriber line internet access subscribers. Chunghwa Telecom sets up modems which have a WiFi-sharing function for its subscribers. It also provides CHT WiFi, which is a public wireless internet service, through the establishment of outdoor access points in payphone booths and through collaboration with supermarkets, fast-food store chains and coffee shop chains to provide indoor wireless internet access. There are over 50,000 WiFi hotspot access points in Taiwan, most of which use the WPA2 encryption mechanism.

The NCC has issued an alert warning advising subscribers to avoid sending confidential or sensitive personal data via WiFi connections and to browse HTTPS websites only. After operators release WiFi access point updates that fix the loopholes, subscribers should apply the updates to their terminal equipment, handsets, tablets or computers as soon as possible. Until the loopholes are fixed, it is recommended that 4G mobile internet access should be used instead.

As of October 20 2017 network operators have not detected any attacks mounted by hackers through such loopholes. However, operators have stated that they are in collaboration with WiFi equipment vendors for firmware and software updates. The NCC is also set to announce information about WiFi equipment suppliers for subscribers when it issues its website software update.

For further information on this topic please contact Arthur Shay at Shay & Partners by telephone (+886 2 8773 3600) or email (arthur@elitelaw.com). The Shay & Partners website can be accessed at www.elitelaw.com.