張貼日期：2017/10/19

[資安漏洞預警通知] WPA2加密協議存在嚴重漏洞，所有含有WPA2加密協議之裝置均可能受影響

主旨：WPA2加密協議存在嚴重漏洞，所有含有WPA2加密協議之裝置均可能受影響

說明：

1. WPA 全稱為 Wi-Fi Protected Access，有 WPA 和 WPA2 兩個標準，是一種保護無線網路安全的加密協議。
2. 比利時研究人員發現WPA2(Wi-Fi Protected Access 2)加密協議中存在嚴重漏洞，包含CVE-2017-13077、CVE-2017-13078、CVE-2017-13079、CVE-2017-13080、CVE-2017-13081、CVE-2017-13082、CVE-2017-13084、CVE-2017-13086、CVE-2017-13087及CVE-2017-13080等。
3. 攻擊者可在含有漏洞的WiFi裝置的有效覆蓋範圍內，攔截使用者傳送的檔案、電子郵件及其他資料等。甚至，特定情況下，攻擊者可以竄改、偽造傳輸的資料，或在正常網頁中植入惡意連結。
4. 影響平臺：所有含有WPA2加密協議之裝置
5. 建議措施：
    1. 請各機關密切注意各家廠商更新訊息，或參考美國Cert/CC官網(http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4)提供之受影響廠商名單，並儘速安裝更新韌體或軟體。
    2. 減少在公共場合使用WiFi服務，減少受害機會。
    3. 使用WPA2之WiFi連線時，應避免於HTTP連線時傳送機敏資料，盡可能使用HTTPS連線作為機敏資訊傳送。
    4. 建議變更WiFi AP之SSID(例如手機所分享之WiFi AP)，避免存在容易讓人識別身分之名稱，以減少遭鎖定攻擊機會。
    5. 可以的話，建議使用有線網路取代無線網路以強化安全。
    6. WiFi服務為區域性連線使用，因此具備良好安全觀念，以及留意安全議題與使用方式，此問題影響程度有限，不須過於恐慌。
6. 參考資料:
    1. https://www.ithome.com.tw/news/117515
    2. https://www.inside.com.tw/2017/10/17/wpa2breaking
    3. https://www.krackattacks.com/

計算機與通訊中心
網路系統組 敬啟