

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2017101808105858	發佈時間	2017-10-18 08:10:00
事故類型	ANA-漏洞預警	發現時間	2017-10-17 00:00:00
影響等級	高		

[主旨說明:]【漏洞預警】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

[內容說明:]

轉發行政法人國家資通安全科技中心 資安訊息警訊 NCCST-ANA-201710-0011

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。

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。

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。

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

[影響平台:]

所有含有 WPA2 加密協議之裝置

[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

[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/>

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：service@cert.tanet.edu.tw