研究人員發表鎖定 Broadpwn 漏洞的 Wi-Fi 蠕蟲

研究人員揭露博通 Wi-Fi 晶片 Broadpwn 漏洞，可偵測裝置發出的 Wi-Fi 探測請求，將裝置引導至惡意 Wi-Fi 熱點，摧毀 Wi-Fi 控制器的記憶體，在不驚動使用者下，持續散布至周遭的裝置。

文/陳曉莉 | 2017-07-31 發表

發現博通（Broadcom）Wi-Fi 晶片上 Broadpwn 安全漏洞的資安研究人員 Nitay Artenstein 上周於黑帽（Black Hat）駭客大會上揭露漏洞細節，並發表首支針對該漏洞的 Wi-Fi 蠕蟲，允許駭客自遠端在智慧型手機的應用處理器上執行任意程式。

博通主宰了智慧型手機的 Wi-Fi 晶片市場，根據 Artenstein 的粗略調查，Samsung Galaxy 從 S3 到 S8、所有的 Samsung Notes3、Nexus5/6/6X/6P，以及 iPhone 5 以後的所有 iPhone 版本，皆採用了博通的 Wi-Fi 晶片，受到 Broadpwn 漏洞影響的晶片型號自 BCM4339 到 BCM4361 不等。

Artenstein 指出，Broadpwn 為一透過可無線區域網路（WLAN）散布的完美漏洞，它既不需認證，也不必仰賴目標裝置提供資訊，並允許駭客將受駭裝置變成行動感染站。

Artenstein 所打造的攻擊程式能夠捕獲目標裝置所發出的 Wi-Fi 探測請求，並將該裝置引導至惡意的 Wi-Fi 熱點，允許駭客傳遞數據以摧毀 Wi-Fi 控制器的記憶體，且完全不驚動使用者，一旦有裝置被感染，它就能持續散布至周遭的裝置。

在 Artenstein 於稠密的城市區域監控一小時後，發現有數百個裝置發出 Wi-Fi 探測請求，其中有 7 成採用 Broadcom 晶片，根據估計，目前全球約有 25 億的智慧型手機用戶，顯示有超過 15 億的智慧型手機遭 Broadpwn 漏洞波及。Google 與蘋果已於今年 7 月分別修補了 Android 與 iOS 平台上的 Broadpwn 漏洞。

資料來源：iThome