資安訊息：五月份網路安全威脅報告

2014/06/17

風險等級： 資安訊息

摘　　要： 資安事件：綜觀本月份資安新聞，可看到眾多新聞呼籲 Windows XP 使用者盡快升級系統，可參考 iThome 發佈「趨勢：網路報稅勿用 XP 電腦、慎防 P2P 軟體」、「後 XP 時代的安全危機第一槍」、「微軟例行性更新，首次 XP 沒得修補！」及大紀元發佈「如何防護 XP 電腦安全」。微軟於 4 月 8 日終止支援 Windows XP 系統，雖然 XP 使用者仍可繼續使用該系統，但仍會持續面臨新的安全風險，建議 XP 使用者盡速升級作業系統，降低受駭威脅。

重大弱點：微軟公佈了 9 項重大更新，Adobe 發布旗下產品(Flash Player /Air /Reader /Acrobat /Illustrator) 共 3 個弱點通告，Apple 發佈旗下產品(Safari /iTunes /OS X Server) 共 3 個弱點通告，Google 發佈 Chrome 瀏覽器共 2 個弱點通告，McAfee 發布 2 個弱點通告，WordPress 發布 13 個弱點通告，Apache 發布 4 個弱點通告，Oracle 發布 13 個弱點通告，Cisco 發佈旗下產品 30 個弱點通告，SUSE 發佈 11 項更新，Red Hat 發布 24 項更新，建議受影響的用戶盡速上網修補。

病毒狀況：防毒軟體廠商近期發現 BKDR_BLADABIN.AB 後門程式，可以執行來自遠端惡意攻擊者的命令，有效地攻擊被感染的系統，並竊取敏感資料。建議您勿瀏覽可疑或惡意網站以及開啟任何可疑的檔案或郵件，並更新防毒軟體病毒碼至最新版本。

網路威脅分析：經由中華電信 SOC 團隊進行網路威脅情報分析後，建議客戶可採取以下防護措施：
(1)為避免遭受 NTP 、SNMP 等 UDP 的 DDOS 等攻擊，建議對各系統限制外部連線 IP ，以避免遭受外部攻擊者掃描與利用 NTP 、SNMP 協定特性對第三方發動攻擊。
(2)針對 IE 0day(CVE-2014-1776) 弱點，建議針對個人電腦進行更新(MS14-021) ，針對伺服器如有使用 IE 瀏覽器，請關閉 IE 瀏覽器 ActiveX 及 Active Scripting 功能，以避免受駭。
(3)針對 OpenSSL 攻擊事件仍有較多之攻擊事件數量，來源國最多為大陸及香港地區，請確認目前所使用之 OpenSSL 版本已更新至無 Heartbleed 弱點，並更換憑證與重新設定用戶密碼。另外，目前 IPS 設備皆以具備防護此類攻擊之能力，建議更新 IPS 至最新版本。

本資訊轉自教育部資安服務網