資通安全網路月報

一、近期政策重點

114 年 9 月 24 日總統公布《資通安全管理法》修正通過，為我國資通安全法制建構邁出關鍵一步。此次修法不僅回應國內外資安環境快速變遷的挑戰，更全面強化政府與社會整體資安韌性，為我國數位國土安全建立更堅實的防護屏障。

二、資通安全趨勢

(一) 我國政府整體資安威脅趨勢

事前聯防監控

本月蒐整政府機關資安聯防情資共 6 萬 5,230 件(減少 2 萬 4,208 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(39%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(25%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(19%)，大多是系統遭未經授權存取或取得系統/使用者權限。統計近 1 年情資數量分布，詳見圖 1。

假陳情、真釣魚：駭客鎖定官方管道發動攻擊

經進一步彙整分析聯防情資資訊，發現近期駭客以「陳情」或「投訴」名義，寄送社交工程釣魚郵件，主要透過政府機關相關陳情管道 (如意見信箱或官方網站) 遞送惡意檔案，企圖誘使收件者或政府機關承辦窗口開啟並執行惡意附件，相關情資已提供各機關聯防監控

防護建議。

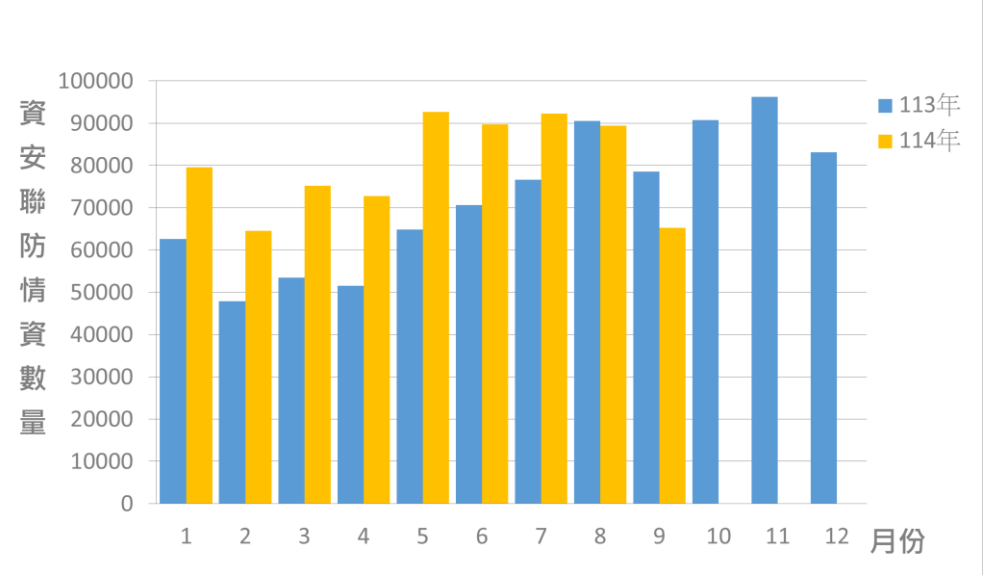

圖 1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共 106 件，較去年同期減少 49.76%，通報類型以非法入侵為主，資安院發現部分機關資訊設備出現 PUBLOAD 惡意程式特徵連線，經機關調查多為隨身碟感染所造成。近 1 年資安事件通報統計詳見圖 2。

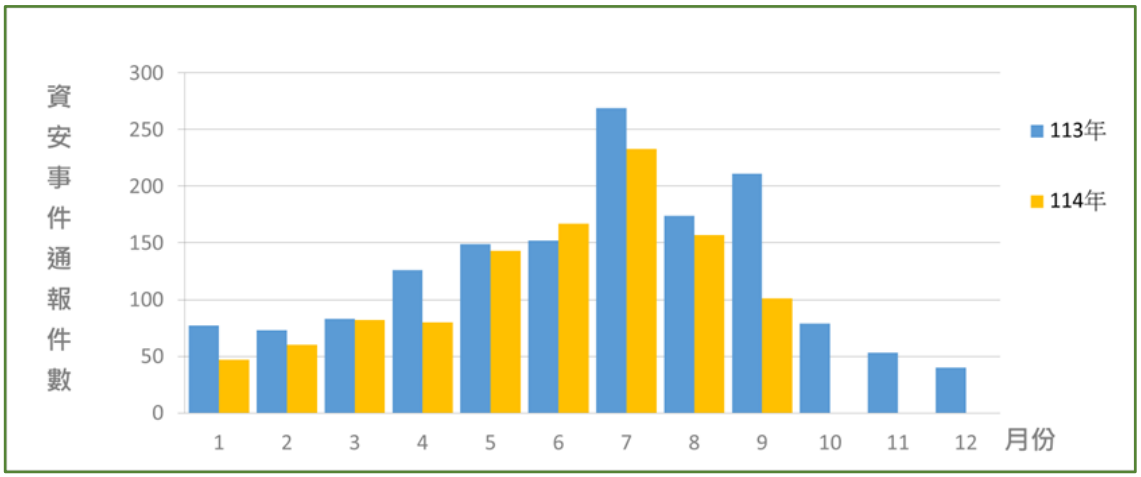

圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	防火牆設備 Cisco 安全防火牆設備的版本存在高風險漏洞 嚴重程度：CVSS 9.0 (CVE-2025-20363)	● Cisco 安全防火牆自適應安全設備(ASA)、Cisco 安全防火牆威脅防禦(FTD)軟體、Cisco IOS 軟體、Cisco IOS XE 軟體和 Cisco IOS XR 軟體的 Web 服務存在重大資安漏洞(CVE-2025-20363)。 ● 此漏洞源於 HTTP 請求對使用者輸入驗證不當，攻擊者可向受影響設備的 Web 服務發送精心設計的 HTTP 請求，以 root 身分執行任意程式碼，從而導致受影響裝置中斷服務。官方已針對漏洞釋出修復更新，請參考官方說明儘速確認並進行修補。
已知遭駭客利用之漏洞	防火牆設備 Cisco 安全防火牆設備的 版本存在高風險漏洞 嚴重程度：CVSS 9.9 (CVE-2025-20333)	● Cisco 安全防火牆自適應安全設備(ASA)和 Cisco 安全防火牆威脅防禦(FTD)的 VPN Web 伺服器中存在重大資安漏洞(CVE-2025-20333，CVSS)。 ● 此漏洞源自伺服器對使用者輸入 HTTP(S)請求驗證不當，持有有效 VPN 使用者憑證的攻擊者，可藉由精心設計的 HTTP 請求，允許經身分驗證的遠端攻擊者以 root 身分在受影響設備執行任意程式碼。官方已針對漏洞釋出修復更新，請參考官方說明儘速確認並進行修補。
	Android 裝置 Android Runtime (ART)	● 研究人員於 Android 發現多個漏洞，公告指出 ART 中存在 use-after-

警訊	類別	內容說明
	Use-After-Free 存在高風險漏洞 嚴重程度：CVSS 9.3 (CVE-2025-48543)	free(記憶體使用後釋放)缺陷，攻擊者可利用此缺陷繞過 Chrome sandbox，向系統層 (system_server) 晉升權限，達成本地提權，且利用時不需額外使用者互動。(CVE-2025-48543)。 ● 漏洞影響 : 攻擊者可以直接利用該漏洞從遠端 (鄰近/相鄰) 執行程式碼，過程中不需要取得其他執行權限，也不必與使用者互動。 ● 官方已針對漏洞釋出修復更新，請參考官方說明儘速確認並進行修補。
	網站應用平台 Web 應用伺服器 Sitecore Experience Manager (XM) 與 Experience Platform (XP) 存在高風險漏洞 嚴重程度：CVSS 9.0 (CVE-2025-53690)	● 研究人員發現 Sitecore XM/XP 在特定版本的 ViewState/反序列化處理存在不安全行為，透過 ViewState 或反序列化不可信資料導致 RCE (CVE-2025-53690)。 ● 若未修補，可能直接導致遠端代碼執行、機密資料外洩或被用作內部跳板 (實務上攻擊者可用來部署後門/偵蒐惡意程式)。 ● 官方已針對漏洞釋出修復更新，請參考官方說明儘速確認並進行修補。

警訊說明：

「漏洞警訊」: 為已驗證漏洞但尚未遭攻擊者大量利用，修補速度建議儘快安排更新。

「已知遭駭客利用之漏洞」: 已知有漏洞成功攻擊情形，建議即刻評估修補

三、近期資安事件分享

小心陳情附件！偽冒 PDF 捷徑檔暗藏惡意程式

國家資通安全研究院發現部分機關資訊設備對外惡意連線，經機關調查顯示入侵來源為官方網站提供之陳情管道，承辦人員為處理陳情案件，將其所附之壓縮檔解壓縮後逐一檢視檔案，執行偽冒 PDF 檔之捷徑(lnk)檔，以致遭植入惡意程式。

經驗學習(Lessons Learned)

國家資通安全研究院發現近期攻擊者透過機關陳情管道（例如意見信箱）投遞夾帶惡意程式之檔案，藉此誘使承辦人員執行惡意程式以達成入侵目的，建議各機關：

1. 強化檔案安全檢驗

由於壓縮檔可能繞過一般檢測機制，建議在解壓縮前先確認檔案名稱與實際格式，避免執行可疑內容，並透過防毒掃描或沙箱測試強化防護。

2. 建立標準化流程

針對外部來源檔案，應制定檢視與風險分級作業準則，並規範於專屬的檢視環境或隔離平台處理，依不同風險層級採取相應的安全措施。

四、國際資安新聞

➢ AI 強化惡意軟體，具備超高隱匿性與迴避能力 (資料來源：Dark Reading)

資安公司趨勢科技（Trend Micro）研究人員追蹤到一個名為「EvilAI」的惡意軟體攻擊活動。該活動利用看似合法的 AI 工具和軟體，來暗中植入惡意程式碼，為未來的攻擊鋪路。目前，該活動已在全球造成數百名受害者，橫跨美國、印度、英國、德國、法國、巴西等多國的製造業、政府、醫療保健及其他產業。

駭客使用名為「App Suite」、「Epi Browser」、「Manual Finder」等應用程式來偽裝惡意軟體，這些程式具備專業的使用者介面與功能，以符合使用者對此類軟體的預期。在大多數的應用程式中，其惡意程式碼皆由 AI 生成，藉此有效規避防毒軟體及威脅偵測工具的掃描。

為了進一步增加這些惡意程式的真實性，駭客從新註冊實體取得的程式碼簽章憑證（code-signing certificates）實行數位簽章。一旦在受害者裝置上執行，EvilAI 應用程式會進行廣泛的偵察，以繪製受害者系統環境的地圖，並識別已安裝的資安產品。完成偵察後，EvilAI 應用程式會強制終止 Microsoft Edge 和 Chrome 等瀏覽器進程，並嘗試停用受害者的資安防護產品。

官方防範建議

FBI 建議，為了防止成為類似詐騙的受害者，使用者應採取多項防範措施，其中一項就是直接在瀏覽器中輸入官方網址 www.ic3.gov，而非透過搜尋引擎點擊連結。

與 Salt Typhoon、UNC4841 相關的 45 個新網域曝光

(資料來源：Silent Push)

資安公司 Silent Push 發現了 45 個新網域，部分最早可追溯至 2020 年，這些網域與中國駭客組織 Salt Typhoon 和 UNC4841 有關，被用於進行網路間諜活動。

這些網域由使用假名和虛假地址的人註冊，讓駭客得以長期且隱密地存取目標組織，特別是電信業。

由於 Salt Typhoon 的攻擊手法具備高度持續性，且其基礎設施與其他中國資助的團體有重疊之處，持續構成威脅。因此，各組織應立即檢查其 DNS 日誌，搜尋與這些網域及 IP 位址相關的活動，以防範潛在的入侵行為。

Salt Typhoon 和 UNC4841 攻擊指標新網域清單請參閱網址: https://www.silentpush.com/blog/salt-typhoon-2025/

五、近期重要資安會議及活動

日期	活動/會議	對象
9 月 24 日	產品資安論壇：共築產品資安責任鏈	產、官、學
9 月 25 日-10 月 27 日	產品資安漏洞獵捕計畫	產