資通安全網路月報

一、近期政策重點

《資通安全管理法》修正草案已於 114 年 8 月 29 日立法院三讀通過，資安署將於總統公布後六個月內完成 8 項子法修訂，期與母法同步施行。另資安署將持續強化防禦架構及即時監控，有效提升網路安全防護及應變能力，並透過法規與政策推動，提升整體防禦韌性。

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 8 萬 9,438 件(減少 2,776 件)，分析可辨識的威脅種類，第 1 名為入侵攻擊類(36%)，大多是系統遭未經授權存取或取得系統/使用者權限；其次為資訊蒐集類(33%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；以及入侵嘗試類(19%)，主要係嘗試入侵未經授權的主機。統計近 1 年情資數量分布，詳見圖 1。

小心有關詢問志工計畫報名之惡意郵件

經進一步彙整分析聯防情資資訊，發現近期駭客利用第三方電子郵件服務(如微軟 Outlook 與 Google Gmail)，以詢問志工計劃報名為由，針對政府機關人員寄送內含惡意附檔之社交工程電子郵件，企圖誘騙收件人開啟惡意附檔以植入後門程式，進而

竊取電腦機敏資訊，相關情資已提供各機關聯防監控防護建議。

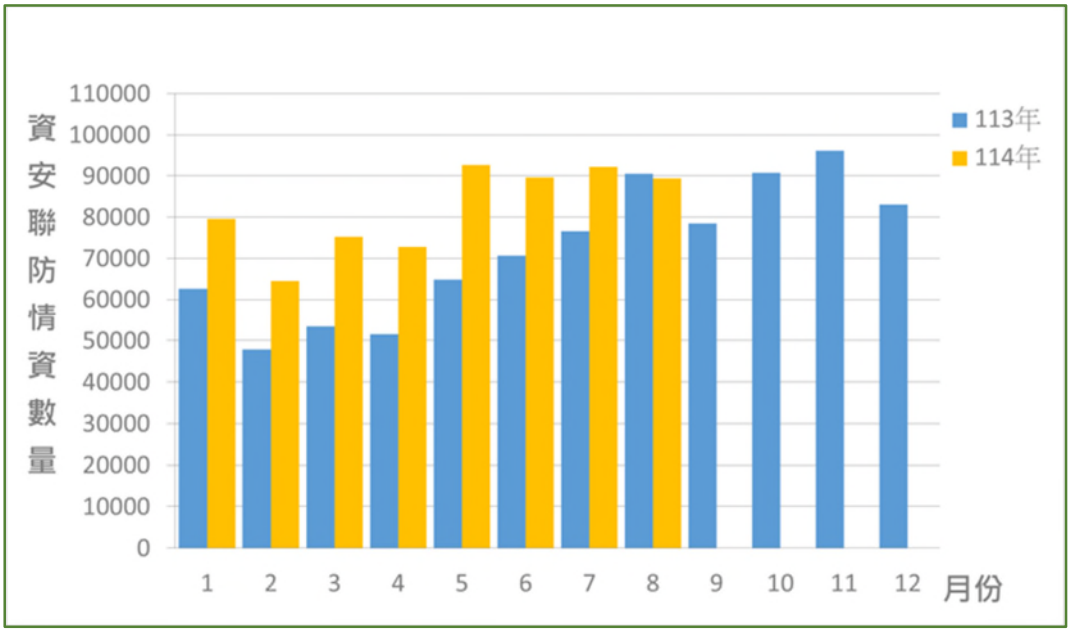

圖 1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共 158 件，較去年同期減少 9.20%，本月實兵演練攻擊成功案件較多，占本月通報件數 53.16%，以注入攻擊為主，其次為加密機制失效與無效的存取控管等事件。近 1 年資安事件通報統計詳見圖 2。

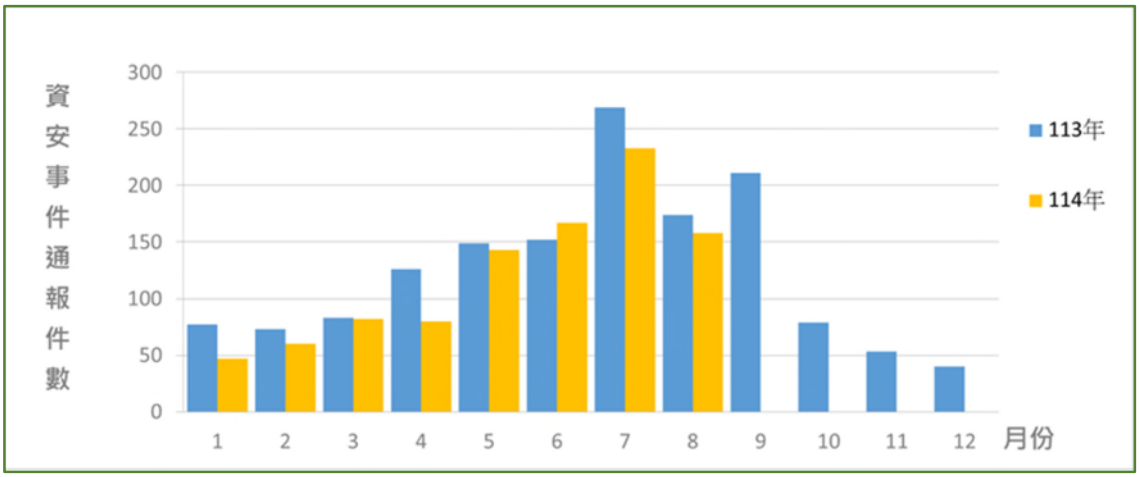

圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	網通設備 Cisco Secure Firewall Management Center (FMC) 嚴重程度：CVSS 10 (CVE-2025-20265)	● Cisco Secure Firewall Management Center (FMC)軟體之 RADIUS 子系統存在未妥善處理特殊字元之注入(Injection)漏洞(CVE-2025-20265)。未經身分鑑別之遠端攻擊者可於憑證輸入階段注入任意 Shell 指令，進而於系統上達成遠端執行任意程式碼。 ● 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。
已知遭駭客利用之漏洞	網通設備 Citrix NetScaler ADC and Gateway 嚴重程度：CVSS 9.2 (CVE-2025-7775)	● Citrix NetScaler ADC 與 NetScaler Gateway 多個版本存在記憶體溢位(Memory Overflow)漏洞(CVE-2025-7775)，未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼或阻斷服務。 ● 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。
	Windows 版本 WinRAR 嚴重程度：CVSS 8.4 (CVE-2025-8088)	● Windows 版本 WinRAR 7.12(含)以前版本，存在路徑穿越(Path Traversal)漏洞(CVE-2025-8088)，未經身分鑑別之遠端攻擊者可利用漏洞製作惡意壓縮檔並透過釣魚信件發送，當受駭者開啟壓縮檔後，惡意程式將寫入開機資料夾中，並於每次開機時自動執行。 ● 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	類別	內容說明
	Trend Micro Apex One 嚴重程度： CVSS 9.4 (CVE-2025-54948 與 CVE-2025-54987	● Trend Micro Apex One 、 2019 Management Server 14039(含)以前版本，本地部署版本存在作業系統指令注入(OS Command Injection)漏洞(CVE-2025-54948 與 CVE-2025-54987)，未經身分鑑別之遠端攻擊者可於管理主控台上傳惡意程式碼並執行，請儘速確認並進行修補。 ● 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

工控設備應變更預設密碼並限制暴露於網際網路

國家資通安全研究院發現部分政府機關使用之工控設備控制頁面，未限制存取且暴露於網際網路，亦未變更登入預設密碼，本月發現其中有遭入侵成功對外連線至殭屍網路(Botnet)之事件，後續機關評估遠端操作為非必要需求，已將該受駭設備下架，後續改由人員至現場手動操作。

經驗學習(Lessons Learned)

政府機關透過工控環境設備來管理業務運作，許多設備可能設置於偏遠地區或環境嚴苛的地點，例如水庫或變電站，無形中增加人工到場維護的成本與資源。因此，許多營運單位傾向於透過遠端操作監控與維護工控設備，以降低維護成本提升作業效

率。然而未能設置完整的防護架構(例如防火牆或存取控管機制)，導致未限制或弱管控的存取狀況時有發生，使得工控設備更容易成為駭客攻擊的目標，進而對產線、公共安全及營運造成重大風險，建議各機關：

1. 建立安全且可監控的遠端存取策略

將遠端存取變得「安全且可監控」，包括白名單管制、設置跳板機或 VPN 連線，避免暴露於公開網路，並配合日誌紀錄記錄操作人、時間與行為等，以持續監控。

2. 落實工控設備帳號安全，從變更預設密碼做起

落實帳號與密碼管理，部分工控設備的預設密碼可透過使用手冊、官方文件或網路論壇查找取得，駭客不需要破解或社交工程，即有機會登入成功，這也是許多自動化工具最常利用的漏洞，建議更換原廠預設密碼，設定具足夠長度與複雜度的密碼，並定期更新。同時遵循最小權限原則，確保僅有授權人員能存取與操作設備境下使用。

3. 立即修補已知漏洞，鞏固營運安全

儘速修補已知弱點，落實弱點管理政策，透過儘速修補已知弱點，不僅能降低設備遭攻擊的可能性，也能確保工控系統持續安全運作，保障營運與公共安全。

四、國際資安新聞

➢ 趨勢科技證實：Apex One 本地部署版存在關鍵漏洞，已被駭客積極利用 (資料來源: SC Media)

趨勢科技（Trend Micro）發布修補程式，以解決其 Apex One 管理主控台（on-premises versions of Apex One Management Console） 本地部署版本中已被駭客利用的關鍵資安漏洞。

這兩個漏洞分別為 CVE-2025-54948 與 CVE-2025-54987，在 CVSS（通用漏洞評分系統）中的嚴重性評分均高達 9.4，屬於管理主控台指令注入(command injection)與遠端程式碼執行(remote code execution）漏洞。

- CVE-2025-54948 漏洞源於管理主控台後端缺乏足夠的輸入驗證，讓遠端攻擊者只要能夠存取管理主控台介面，就能植入惡意作業系統指令，進而執行遠端程式碼。
- CVE-2025-54987 漏洞與前者類似，但針對不同的 CPU 架構。

一般而言，駭客需具備實體或遠端存取權限，並能登入至 Trend Micro Apex One 管理主控台，才能利用這些漏洞。趨勢科技已針對本地部署版本釋出一個臨時修補程式(fix tool)，而正式的修補程式預計將在八月中旬發布。

➢ 美英日等 13 國聯合警告，中國國家級駭客滲透全球關鍵基礎設施 (資料來源 Bleeping Computer)

根據美國國家安全局(NSA)、英國國家網路安全中心(NCSC ）及其他國家的合作夥伴發布的聯合公告，「鹽颱風」(Salt Typhoon) 的網路間諜行動與三家位於中國的科技公司有關聯，這三家公司分別是四川聚信和網路科技有限公司、北京寰宇天穹資訊科技有限公司和四川智信瑞傑網路科技有限公司，並為中國國家安全部和解放

軍提供網路產品與服務。

該駭客組織並非依賴零時差漏洞，而是利用網路邊緣設備上早已廣為人知且已修復的漏洞進行攻擊，「鹽颱風」過去曾入侵過 AT&T、Verizon、Lumen 等多家公司。

主要利用已知漏洞針對各國的重要設施建立後門以蒐集情報，對象涵蓋各國電信、政府、交通及軍事基礎設施，建議優先修補 CVE-2024-21887 (Ivanti)、CVE-2024-3400 (Palo Alto)、CVE-2023-20273 (Cisco)、CVE-2023-20198 (Cisco)及 CVE-2018-0171 (Cisco)等已知漏洞，強化網路設備的安全性，加強對日誌的監控，若採用思科 (Cisco)設備，應即停用 Smart Install 與 Guest Shell。

五、近期重要資安會議及活動

日期	活動/會議	對象
9 月 24 日	資安院 9 月 24 日舉辦產品資安論壇與產官學研共築產品資安責任鏈	產、官、學