資通安全網路月報

一、近期政策重點

資通安全法修正案已於 114 年 9 月 24 日經總統公布，並於 114 年 12 月 1 日施行；其相關子法「資通安全法施行細則」、「資通安全責任等級分級辦法」、「資通安全維護計畫實施情形稽核辦法」、「資通安全事件通報應變辦法」、「公務機關所屬人員辦理資通安全事項作業辦法」、「資通安全情資分享辦法」及「危害國家資通安全產品審查辦法」等 7 項子法，預計於 115 年 1 月 1 日施行。

二、近期資安事件分享

案例 1

偽冒 Chrome 元件更新提示，不慎誤點遭入侵

機關辦理資安健診時，偵測到一台電腦存在可疑程式，經 SOC 鑑識研判該程式屬高風險檔案，且偵測發現異常對外連線行為。經查肇因於人員於下班時間使用辦公室電腦瀏覽網頁時，出現引導使用者更新 Chrome 擴充元件的彈跳視窗，人員誤信該提示為正常更新通知，遂依指示操作以致下載惡意程式。後續機關已將受駭設備重新安裝作業系統，並同步規劃進行教育訓練，提升使用者資安意識。

經驗學習(Lessons Learned)

近年駭客透過偽裝系統更新或瀏覽器擴充元件更新的彈跳視

窗，誘使使用者在相似的介面下載惡意程式，若缺乏瀏覽器或端點防護機制有效控管，即可能成為惡意程式進入端點的入口。機關可透過強化瀏覽器控管、限制未授權擴充元件與程式執行，以及提升使用者辨識能力等方式，降低遭假更新誘導下載惡意程式的風險。

源頭管理軟體安裝，採白名單並啟用阻擋彈窗

強化瀏覽器與擴充元件管控：採白名單制度、啟用彈跳視窗阻擋，並集中由管理者派送瀏覽器與擴充元件更新，降低使用者接觸偽造更新提示的風險。

嚴管軟體執行權限，杜絕異常程式活動

限制未授權程式與異常行為：透過群組原則(GPO)阻擋未簽章或來源不明的程式執行，並以白名單方式分層控管，兼顧業務需求與防護效果。

提升人員資安意識，辨識偽冒陷阱

提升使用者辨識能力：加強教育訓練，使人員能辨識假更新提示、偽造下載頁面與可疑彈窗，降低誤點與安裝惡意程式的可能。

案例 2

公私混用又弱密碼遭破，導致社群公務帳戶被接管

機關基於業務宣傳需求設置 Facebook 粉絲專頁，並由業務承辦人與維運廠商負責日常管理作業。惟承辦人之個人 Facebook 帳號因使用弱密碼遭不明人士入侵，進而影響與個人帳號綁定之機關粉絲專頁管理權限，致原管理者們(承辦人及維運廠商)皆遭移除管理權限。後續報請內政部警政署刑事警察局聯繫 Meta 公司，協助恢復原管理者權限後，立即要求承辦人員與維運廠商變更密

碼、再次清查帳號及確認 Facebook 相關安全要求設定。

經驗學習(Lessons Learned)

公務粉絲專頁不宜使用個人帳號進行管理，因個人帳號除可能連動第三方應用程式、跨裝置登入、密碼跨平台重複使用、未啟用多因子驗證或因個人習慣導致安全設定不一致，均可能提高帳號遭入侵或存取權杖(Access Token)遭濫用的風險，故建議強化帳號安全控管、控管連動應用程式及定期檢視。

啟用多因子驗證並開啟安全設定

(1) 啟用多因子驗證 (MFA, Multi-Factor Authentication)。
(2) 使用高強度且不重複的密碼，並建立定期更換機制。
(3) 啟用「登入提醒」(Login Alerts)，並定期檢查「安全性與登入」的登入地點、已登入裝置與授權瀏覽器。
(4) 啟用「受信任裝置管理」，降低帳號被未授權登入的風險。

定期檢查已授權或連動之應用程式

(1) 定期檢查 Facebook「應用程式與網站」中已授權的第三方 App。
(2) 移除不明或不再使用的應用程式，以避免 OAuth Token 遭濫用。
(3) 監控與粉專相關的外部工具(如社群排程系統或廣告管理應用程式)的授權情形，降低因 Token 失竊而被操作粉專的風險。

三、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 2,795 件(增加 4,174 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(41%)，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(23%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(18%)，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。

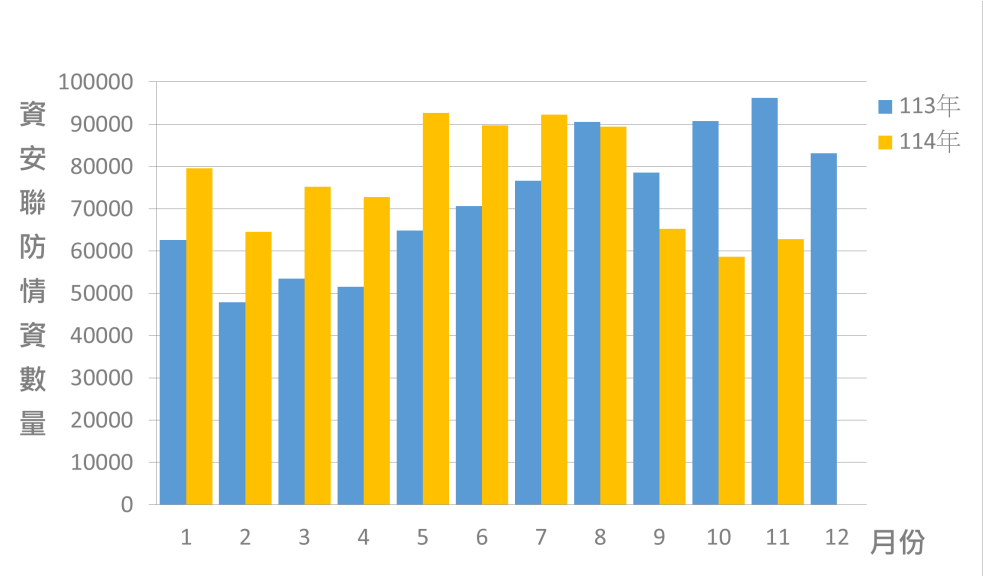

圖 1 資安聯防監控資安監控情資統計

駭客把病毒藏在合法網站躲避檢查

經進一步彙整分析聯防情資資訊，發現近期駭客於社交工程釣魚郵件中濫用免費雲端分享空間 CatBox 作為惡意程式下載站。該網站為免費之雲端分享空間，提供使用者上傳檔案並產生下載連結，以供檔案存取或分享。惟駭客藉由利用其合法網域散布惡意程式，以規避資安偵測機制，相關情資已提供各機關聯防監控防護建議。

事中通報應變

本月資安事件通報數量共 72 件，較去年同期增加 35.85%，通報類型以非法入侵為主，占本月通報件數 58.40%，仍有機關因可攜式媒體感染 PUBLOAD 惡意程式；此外，亦觀察到有機關網路錄影機(Network Video Recorder, NVR)遭入侵利用 Curl 指令下載 Linux 惡意程式。近 1 年資安事件通報統計詳見圖 2。

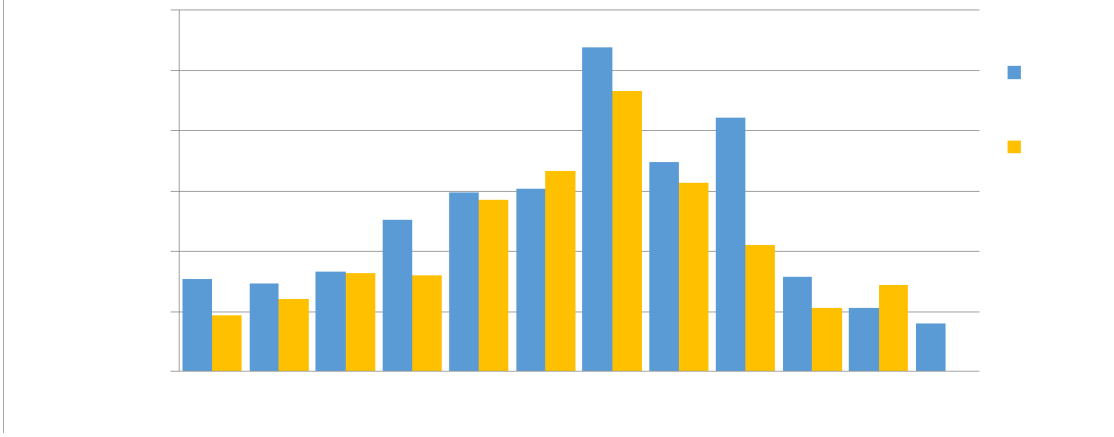

圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	用戶/伺服器軟體 Samba 存在遠端指令執行漏洞 嚴重程度：CVSS 10 (CVE-2025-10230)	• 研究人員發現 Samba 存在作業系統指令注入漏洞(OS Command Injection)漏洞(CVE-2025-10230)。 • 若使用者架設 Samba AD Domain Controller 伺服器並啟用 WINS 協定支援，未經身分鑑別之遠端攻擊者可注入任意作業系統指令於 Samba 伺服器上執行。 • 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
	網通設備 ASUS DSL 路由器存在高風險安全漏洞 嚴重程度：CVSS 9.3 (CVE-2025-59367)	• 研究人員發現 ASUS 部分 DSL 型號路由器存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2025-59367)。 • 未經身分鑑別之遠端攻擊者可透過此漏洞，對受影響設備執行未經授權之存取，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。
	網路管理平台 Cisco Catalyst Center 虛擬設備存在高風險安全漏洞 嚴重程度：CVSS 8.8 (CVE-2025-20341)	• 研究人員發現 Cisco Catalyst Center 虛擬設備存在不當存取控制(Improper Access Control)漏洞(CVE-2025-20341)。 • 取得一般權限之遠端攻擊者可透過傳送特製 HTTP 請求至受影響設備以執行未經授權之修改，進而提升至管理者權限。 • 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 Fortinet FortiWeb 存在路徑遍歷遠端程式碼執行漏洞、作業系統命令注入漏洞 嚴重程度：CVSS 9.8、CVSS 7.2 (CVE-2025-64446 、CVE-2025-58034)	• 研究人員發現 Fortinet FortiWeb 存在相對路徑遍歷(Relative Path Traversal)漏洞(CVE-2025-64446)及作業系統命令注入漏洞(CVE-2025-58034)。 • 未經身分鑑別之遠端攻擊者可透過傳送特製 HTTP、HTTPS 請求，或命令列介面(CLI)指令，進而於受影響設備上執行管理者權限之指令，或執行未經授權的程式碼。 • 官方已針對漏洞釋出修復更新，請參考

警訊	類別	內容說明
		下列官方說明儘速確認並進行修補。 • 參考資料：https://www.fortiguard.com/psirt/FG-IR-25-910 • https://www.fortiguard.com/psirt/FG-IR-25-513
	伺服器/應用程式 Oracle Fusion Middleware 權限提升漏洞 嚴重程度：CVSS 9.8 (CVE-2025-61757)	• 研究人員發現 Oracle Fusion Middleware 存在關鍵功能驗證缺失漏洞(CVE-2025-61757)，允許未經驗證的遠端攻擊者接管身分管理系統。 • 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

四、國際資安新聞

➢ CISA: 勒索軟體團夥正在利用 Linux 高風險漏洞 (資料來源：Bleeping Computer)

CISA 確認，Linux 核心中的高風險權限提升漏洞 CVE-2024-1086 已被勒索軟體團夥利用。 CVE-2024-1086 於 2024 年 1 月 31 日揭露，是 netfilter: nf_tables 核心元件中的一個釋放後使用 (use-after-free) 漏洞。成功利用該漏洞的攻擊者可以利用本機存取權限提升目標系統的權限，甚至可能取得受感染裝置的 root 權限。據 Immersive Labs 稱，攻擊者獲得 root 權限後，可能會進行系統接管、橫向網路移動和資料竊取。此漏洞影響主流 Linux 發行版，包括 Debian、Ubuntu、Fedora 和 Red Hat，涉及核心版本 3.15 至 6.8-rc1。該漏洞先前於 2024 年 5 月被添加到已知可

利用漏洞（KEV）目錄中，最近的更新報告顯示，該漏洞目前正被用於勒索軟體攻擊活動。

- **英國國家醫療服務體系 (NHS) 英格蘭分部警告：7-Zip 漏洞正被積極利用 (CVE-2025-11001)**
  (資料來源：Help Net Security)

英國國家醫療服務體系 (NHS) 英格蘭分部警告:7-Zip 漏洞正被積極利用 (CVE-2025-11001)

英國國民保健署 (NHS) 英格蘭分署數位部門發布警告，指出 7-Zip 漏洞 CVE-2025-11001 正被攻擊者利用。 CVE-2025-11001 最初在 7-Zip v21.02 版本中引入，是一個路徑/目錄遍歷漏洞，已於 7 月在 7-Zip v25.00 版本中與 CVE-2025-11002 一起修復。CVE-2025-11001 存在於 ZIP 檔案中符號連結的處理機制中，惡意建構的 ZIP 檔案資料會導致程式遍歷到非預期目錄。攻擊者可以利用此漏洞以服務帳戶的身份執行程式碼。研究人員「PacBypass」指出，CVE-2025-11001 漏洞僅在 Windows 系統上可被利用，且僅可透過具有管理員權限的使用者/服務帳戶或啟用了開發者模式的 Windows 電腦進行攻擊。由於 7-Zip 軟體不具備自動更新功能，因此強烈建議 7-Zip 用戶盡快升級至最新版本。目前尚不清楚這些攻擊是定向的還是普遍存在的。

五、 近期重要資安會議及活動

日期	活動/會議	對象
12 月 18 日	行政院國家資通安全會報第 46 次委員會議	會報委員、政府機關