資通安全網路月報

一、資安長話短說

1. AI 引發的自動化漏洞挖掘風暴

當前資安威脅已進入「AI 對抗人類」的不對稱戰爭，以 Anthropic Claude Mythos 與 OpenAI GPT-5.5 為首的新興 AI 模型，展現了超越傳統弱掃工具的深度邏輯推理能力。

(1)全平台覆蓋：短時間內在主流作業系統與瀏覽器中挖掘出數千個高嚴重性漏洞，利用成功率高達 72%。

(2)挖掘深度前所未見：找出隱藏長達 27 年之久的系統底層漏洞（如 OpenBSD 案例），這代表過去被視為「穩定、安全」的老舊核心系統，在 AI 面前已無所遁形。

(3)攻擊武器化加速：將複雜的程式碼邏輯轉化為可立即執行的攻擊指令，大幅縮短了從「發現漏洞」到「發動攻擊」的研發週期。

2. 當漏洞利用時間早於揭露時間

各機關必須正視一個殘酷的現實，傳統的漏洞修補週期（Patching Cycle）已無法應對 AI 的速度，根據「零日漏洞時鐘(Zero Day Clock)」的追蹤，漏洞從揭露到被武裝化的中位數時間，已從 2018 年的 771 天，縮減至

2024 年的 4 小時。進入 2026 年，我們更面臨「漏洞利用早於揭露」的嚴峻挑戰，這意味著當你收到更新通知時，攻擊可能早已發生；此外，過去因利用難度高、被列為低優先順序的「冷門漏洞」或「閒置系統」，現在皆能被 AI 自動化重新組合並利用。

3. 戰略思維從「預防被打」轉向「迅速復原」

面對 AI 自動化、規模化且低成本的攻擊，資安防護的核心邏輯必須進行典範轉移（Paradigm Shift），過往的「絕對不會被駭」是不切實際的幻覺，真正的安全在於「韌性（Resilience）」，資安資源的投入比例，應從單純的「外部阻斷（Prevent）」轉向偵測（Detect）、應變（Respond）與復原（Recover）。

4. 策略、管理與技術的同步進化

針對前面所講的各種威脅趨勢，建議各機關依據下列三維度重新檢視資安體制：

(1)策略面—提升漏洞管理層級：由經營層或政府機關首長親自督導，明確指定資安治理權責。將資安資源從單一的預防投入，調整為涵蓋預防、偵測、應變、復原的整體韌性投資。

(2)管理面—定期演練復原能力、最小權限原則：企業與政府機關應隨時確保業務資料有可離線、可還原的備份，並加強營運持續計畫(BCP)演練，並落實最低權限原則。

(3)技術面—以縱深防禦縮短偵測與反應時間：優先修補對外系統的公共漏洞和暴露(CVE)，在資安管控上，全面啟用多因子鑑別(MFA)與採用建立於 FIDO2 標準的 Passkey 憑證技術，並停用非必要的對外服務與測試介面等。

5. 回歸基本功，以速度應對速度

儘管新興 AI 改變了攻擊的「速度」與「規模」，但其本質仍是利用系統弱點與權限管理疏失，並未改變資安的基本原則，網路縱深防禦、漏洞管理、嚴謹的身分識別等核心做法依然是不變的真理。各機關必須立刻採取行動，重新評估自身資安風險及重新排序漏洞修補清單，並將「平均復原時間（MTTR）」作為衡量資安成效的重要標準，建立起快速反應與修復的韌性體系。

二、近期政策重點

依據資通安全管理法相關子法規定，數位發展部於 115 年 4 月 7 日公告委任資通安全署辦理資通安全相關業務，包含：

1. 資通安全維護計畫實施情形之稽核、改善報告之提出及其他相關事項。
2. 資通安全情資分享、獎勵及其他相關事項。

3. 資通安全事件之通報、應變、演練作業及其他相關事項。
4. 公務機關所屬人員辦理資通安全事項之適任性查核、資安職能訓練、調度支援、獎懲作業及其他相關事項。

三、近期資安事件分享

委外人員下載受駭套件致設備遭植入惡意程式事件

某機關接獲國家資通安全研究院警訊通知，發現資訊設備對外連線至可疑惡意中繼站，經研判與近期 Axios NPM 供應鏈攻擊事件相關。經查，事件係委外廠商駐點人員因專案開發需求使用個人筆記型電腦下載並安裝受影響之第三方套件所致，因該套件官方發布版本已遭植入惡意程式，致設備於安裝後受駭，另因該駐點人員甫到任，尚未實際參與開發專案，經評估暫無專案程式碼、憑證、API 金鑰等資訊外洩之疑慮。

經驗學習(Lessons Learned)

供應鏈攻擊可能使原本可信的官方發布與更新管道遭到利用，攻擊者將惡意程式置入正常更新或安裝流程，使用者即使循正式管道取得套件，仍可能遭受影響，對使用者而言不易於事前辨識或防範。因此，此類事件之防護重點，除持續關注套件來源與異常行為外，更應著重於損害控制，避免單一設備受駭後進一步擴大至內部網路、帳號憑證或其他系統環境。建議機關從下列面向持續強化防護作為：

1. 落實開發與測試環境之區隔與控管：開發或測試環境應儘量與正式環境

區隔，並限制其可存取之系統、資料與憑證範圍，以降低單一主機受駭後之擴散風險。

2. 納管委外廠商設備與連線環境：應依業務需求妥善規劃網路網段與區域，明確規範委外設備之使用環境、網路存取範圍及必要安全設定，以降低影響範圍。

3. 強化開發環境敏感資訊盤點與外洩影響評估：供應鏈攻擊若發生於開發或測試環境，應同步評估是否涉及專案程式碼、API 金鑰、憑證或環境變數外洩風險，並將敏感資訊盤點、權限檢視及必要更換作業納入事件應變處置，以降低後續濫用風險。

四、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 9,246 件(較上月增加 1 萬 6,153 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(61%)，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(18%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(9%)，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。

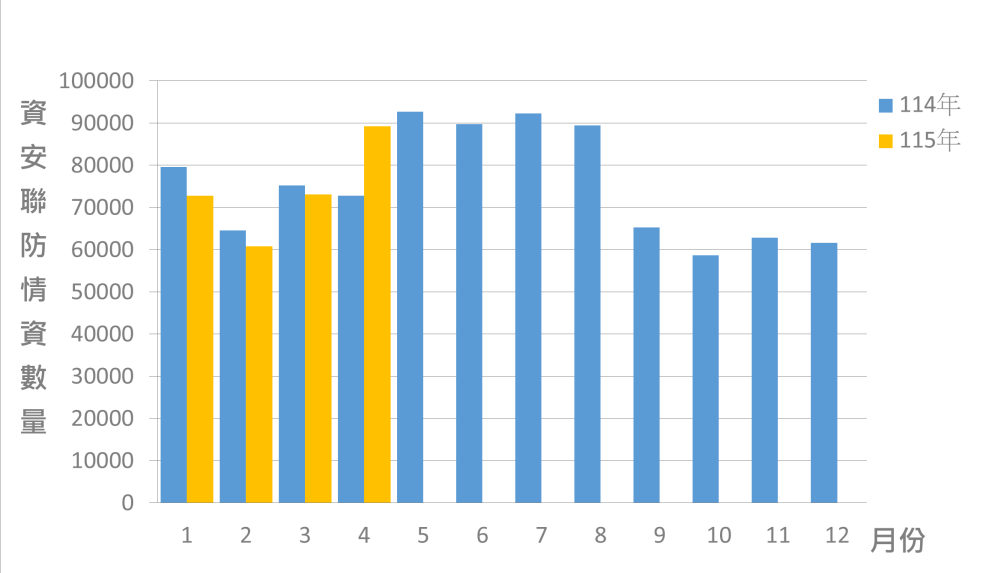

圖 1 資安聯防監控資安監控情資統計

駭客濫用免費圖片分享空間作為惡意檔案散布平台

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攻擊當中，濫用免費圖片託管與分享空間 PNG UP 作為惡意檔案下載站。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 67 件(包含攻防演練數量 18 件)，為去年同期的 0.84 倍，通報類型以非法入侵為主，占本月通報件數 65.67%。本月開始執行網路攻防演練作業，其中發現弱點以預設密碼等「不安全的組態設定」類型占大宗。近 1 年資安事件通報統計詳見圖 2。

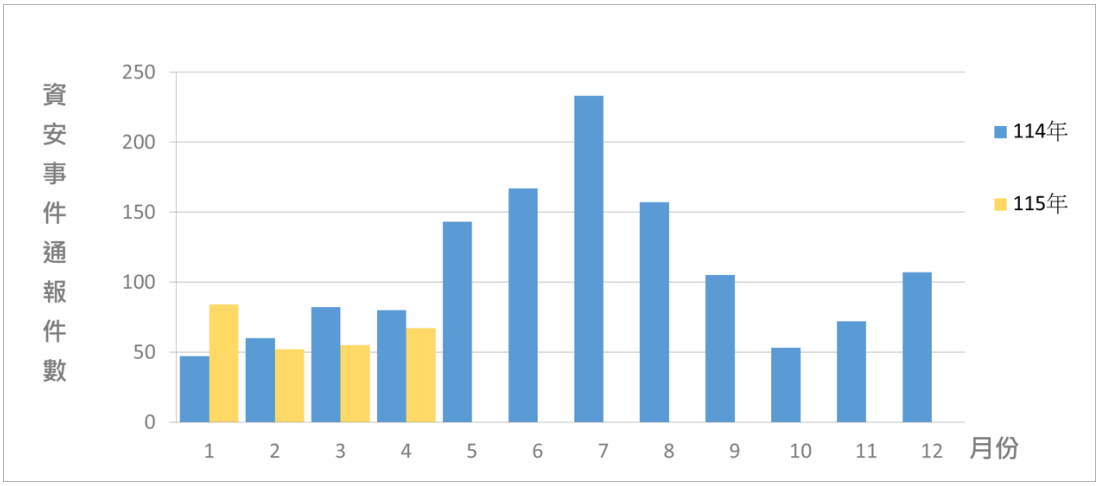

圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	網路儲存系統 QNAP 作業系統 嚴重程度： (CVE-2025-66277： CVSS 9.8)	● 研究人員發現 QNAP 作業系統存在連結追蹤 (Link Following) 漏洞 (CVE-2025-66277)。 ● 未經身分鑑別之遠端攻擊者可利用此漏洞存取未授權之檔案系統路徑。 ● 官方已提供安全公告與修補建議，請儘速更新至 QNAP 公告之修補版本。
	軟體授權管理系統 Cisco Smart Software Manager On-Prem	● 研究人員發現 Cisco Smart Software Manager On-Prem 存在執行任意程式碼(RCE)漏洞(CVE-2026-20160)。 ● 未經身分鑑別之遠端攻擊者可透過對暴露

警訊	類別	內容說明
	嚴重程度： (CVE-2026-20160：CVSS 9.8)	內部服務之 API 發送特製請求，於底層作業系統以 root 權限執行任意命令。 ● 官方已提供安全公告與修補建議，請儘速更新至 Cisco 公告之修補版本。
	路由器 Juniper JSI vLWC 與 Junos OS MX 系列路由器 嚴重程度： (CVE-2026-33784：CVSS 9.8) (CVE-2026-33785：CVSS 8.8)	● 研究人員發現 Juniper JSI vLWC 與 Junos OS MX 系列路由器存在高風險安全漏洞(CVE-2026-33784 與 CVE-2026-33785)。 ● CVE-2026-33784 為預設密碼使用漏洞，未經身分鑑別之遠端攻擊者可使用預設帳密登入系統並取得設備完整控制權；CVE-2026-33785 則可能使低權限本機端使用者於未授權情形下執行高權限 CLI 指令。 ● 官方已發布 vLWC 安全公告，請儘速更新至 3.0.94(含)以上版本。 ● Junos OS MX 系列亦請依官方公告更新至修補版本。
已知遭駭客利用之	網頁瀏覽器 Chromium 為基礎之	● CISA 已將 CVE-2026-5281 列入 KEV 清單，Google 亦表示該漏洞已遭實際利用。

警訊	類別	內容說明
漏洞	瀏覽器 嚴重程度： (CVE-2026-5281： CVSS 8.8)	● 該漏洞為 Dawn 元件使用釋放後記憶體(Use After Free)漏洞，遠端攻擊者可藉特製 HTML 頁面於特定條件下執行任意程式碼。 ● 建議儘速更新 Google Chrome 版本，並同步確認 Microsoft Edge、Brave、Vivaldi、Opera 等相關瀏覽器更新狀態。
	端點管理系統 FortiClient EMS 嚴重程度： (CVE-2026-21643： CVSS 9.8) (CVE-2026-35616： CVSS 9.8)	● CISA 已將 CVE-2026-21643 列入 KEV 清單，Fortinet 亦指出 CVE-2026-35616 已遭實際利用。 ● FortiClient EMS 存在 SQL 注入(SQL Injection)與不當存取控制(Improper Access Control)漏洞，未經身分鑑別之遠端攻擊者可透過特製 HTTP 請求或 crafted requests 執行未授權程式碼或命令。 ● 官方已提供安全公告與修補建議，請儘速更新至 Fortinet 公告之修補版本
	通訊設備 Cisco Catalyst SD-	● CISA 已將 Cisco Catalyst SD-WAN Manager 三項漏洞(CVE-2026-20122、

警訊	類別	內容說明
	WAN Manager 嚴重程度： (CVE-2026-20122： CVSS 5.4) (CVE-2026-20128： CVSS 7.5) (CVE-2026-20133： CVSS 7.5)	CVE-2026-20128、CVE-2026-20133)列入 KEV 清單。 ● 漏洞類型包含不當使用特權 API、可回復格式儲存密碼與敏感資訊揭露，可能導致任意檔案覆寫、取得 DCA 權限或讀取底層系統敏感資訊。 ● 官方已提供安全公告與修補建議，請儘速更新至 Cisco 公告之修補版本。

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

五、國際資安新聞

OpenAI 遭北韓駭客組織利用 Axios 供應鏈攻擊

(資料來源：Security Week)

115 年 4 月 10 日 OpenAI 報告稱其廣泛使用的 Axios JavaScript HTTP 用戶端程式庫近期遭到 Axios 供應鏈攻擊，這次攻擊被歸咎於北韓駭客組織 UNC1069，包括 OpenAI 在內的多家機構受到影響。3 月下旬，攻擊者攻破一位 Axios 維護者的 NPM 帳戶，並發布惡意軟體包，這些軟體包會在 Windows、macOS 和 Linux 系統上安裝跨平臺遠端存取木馬(RAT)。

OpenAI 發現其 macOS 應用程式簽章工作流程執行被入侵的 Axios 軟體包，這可能導致其軟體簽章憑證和公證資料外洩。OpenAI 沒有發現憑證被濫用的證據，但主動吊銷並輪換了憑證，並停止使用舊憑證。

微軟：CISA 將 8 個已被利用的漏洞添加到已知漏洞目錄 (KEV) 中，並設定 2026 年 4 月至 5 月的聯邦最後期限
(資料來源：The Hacker News)

CISA 已將 8 項遭實際利用的漏洞新增至其「已知遭利用漏洞目錄」（Known Exploited Vulnerabilities, KEV），其中包含 Cisco Catalyst SD-WAN Manager 的 3 項漏洞。本次新增漏洞包括：PaperCut NG/MF 的身分驗證漏洞 CVE-2023-27351（CVSS：8.2）、JetBrains TeamCity 的路徑遍歷漏洞 CVE-2024-27199（CVSS：7.3）、Kentico Xperience 的路徑遍歷漏洞 CVE-2025-2749（CVSS：7.2），以及 Synacor Zimbra Collaboration Suite 的跨站腳本（XSS）漏洞 CVE-2025-48700（CVSS：6.1）等。另 Cisco Catalyst SD-WAN Manager 的 CVE-2026-20122（CVSS：5.4）、CVE-2026-20128（CVSS：7.5）及 CVE-2026-20133（CVSS：6.5）等漏洞，可能導致攻擊者上傳惡意檔案、提升權限及洩露敏感資訊。Cisco 指出，其中 CVE-2026-20122 與 CVE-2026-20128 自今年 3 月起已遭實際利用。

CISA 表示，由於相關漏洞具高度資安風險，已要求聯邦機構須於 4 月

23 日前完成 Cisco 相關漏洞修補，並於 5 月 4 日前完成其餘漏洞之修補作業。

防範中國駭客控制網通設備，發動網路攻擊
(資料來源：NCSC)

英國國家網路安全中心（NCSC-UK）發布報告指出，與中國有關聯之攻擊者利用受害 SOHO（小型/家用辦公室）路由器與物聯網(IoT)設備組成隱蔽網路（Covert Networks）發動攻擊，由於 IP 與節點變化快速，傳統以駭侵指標(IoC, Indicators of Compromise）為基礎進行封鎖逐漸失效。該類網路可用於偵察、惡意程式散布、指揮控制及資料竊取，增加政府與關鍵基礎設施遭攻擊風險。

該報告建議各組織應盤點網路邊緣設備與虛擬私有網路（VPN）流量、導入動態威脅情資及遠端存取多重要素驗證(MFA, Multi-Factor Authentication)；高風險組織則應進一步採行零信任架構、IP 白名單、設備憑證驗證，以及利用機器學習與威脅獵捕，主動偵測可疑流量，以降低隱蔽網路攻擊風險。

六、近期重要資安會議及活動

日期	活動/會議	對象
6 月 16 日	NISAC 技術交流會議	NISAC 會員