資通安全網路月報

一、近期政策重點

資通安全管理法修正案已於 114 年 12 月 1 日正式施行，本部業依資安法第 11 條第 3 項之授權，於 114 年 12 月 19 日以數授資法字第 1145000392 號令訂定發布「危害國家資通安全產品審查辦法」，並溯及至 114 年 12 月 1 日施行；另於本部資通安全署官網「資安法規專區」(https://moda.gov.tw/ACS/laws/regulations/18146)公布提報危害國家資通安全產品情資相關表單。

立法院 114 年 12 月 23 日三讀通過《人工智慧基本法》，旨在促進以人為本之人工智慧研發與人工智慧產業發展，建構人工智慧安全應用環境，落實數位平權並保障人民基本權利。本法將確保技術應用符合社會倫理，維護國家文化價值及提升國際競爭力，奠立法制基礎。

二、近期資安事件分享

SSL VPN 漏洞遭利用植入資料庫惡意程式

機關網站偵測發現異常連線，經調查駭客利用 SSL VPN 功能漏洞，成功登入並新增帳號，後續連線至資料庫主機植入惡意程式，過程中發現存在多個資安風險，包括防火牆韌體版本未更新、入侵防禦授權逾期，及管理頁面未限制連線來源等，機關已中斷設備網路進行鑑識與應變處置。

經驗學習(Lessons Learned)

本案事故根因聚焦於「資安授權過期」、「韌體與弱點維護疏漏」、「帳號權限管理缺失」及「外部存取控管過於寬鬆」等四大面向 。由於防護設備韌體未及時更新，致使攻擊者得以利用已知漏洞並配合概念驗證(PoC)工具，成功繞過身分驗證機制進入系統，隨後透過非法新增帳號植入惡意程式 。為防範類似威脅再次發生，提供以下防護作為供各機關參酌：

1. 確保資安防護持續有效

建立授權到期預警機制，確保資安設備(如 IPS 及 Web Filter)維持有效授權，以利自動更新特徵碼以因應資安威脅。

2. 更新韌體與弱點補強

資安設備韌體應納入定期更新排程，並檢查已知弱點修補情形。

3. 帳號控管原則

定期清查系統帳號是否有異常新增，停用或移除未使用之服務功能與帳號。

4. 落實遠端存取之限制

遠端連線服務(如 SSL VPN、SSH)應遵循行政院院臺護字第 1100165761 號公文所述原則「原則禁止、例外允許」及「最小權限原則」方式辦理。

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 1,580 件(減少 1,215 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(45%)，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(21%)，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

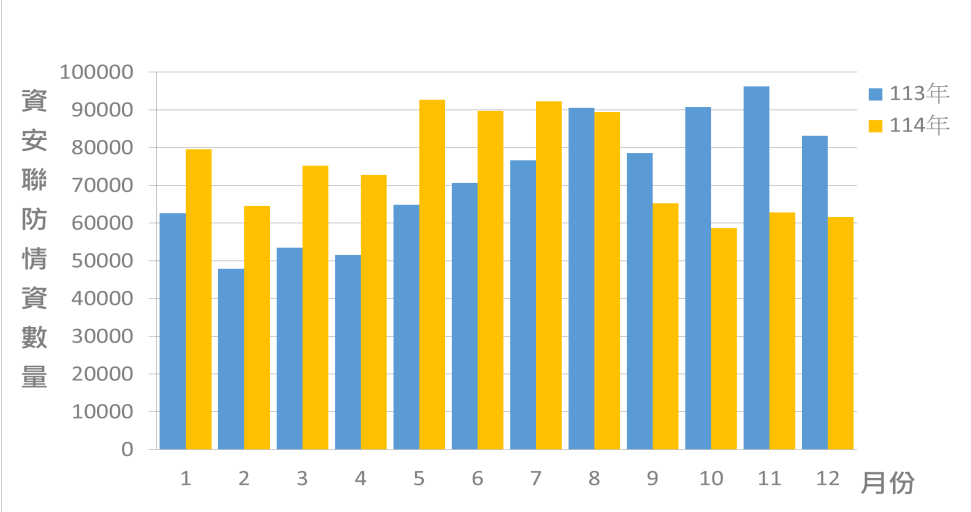

圖 1 資安聯防監控資安監控情資統計

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利用微軟 CAB（Cabinet）檔案作為惡意程式之散布載體。CAB 是微軟常用之壓縮封裝格式，可將多個檔案進行打包並壓縮，並廣泛應用於 Windows 更新、驅動程式及安裝程式之部署流程。惟因其具備封裝彈性與合法性，亦常遭駭客濫用以隱匿惡意內容或降低檔案特徵可見度。駭客將惡意執行檔藏匿於 CAB 檔中，以繞過安全偵測並誘使收件者點擊執行惡意內容，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 107 件，是去年同期的 1.67 倍，通報類型以非法入侵為主，占本月通報件數 71.57%。本月份再次偵測到多個機關，因安裝冒牌軟體以致植入惡意程式占總通報件數 32.71%。近 1 年資安事件通報統計詳見圖 2。

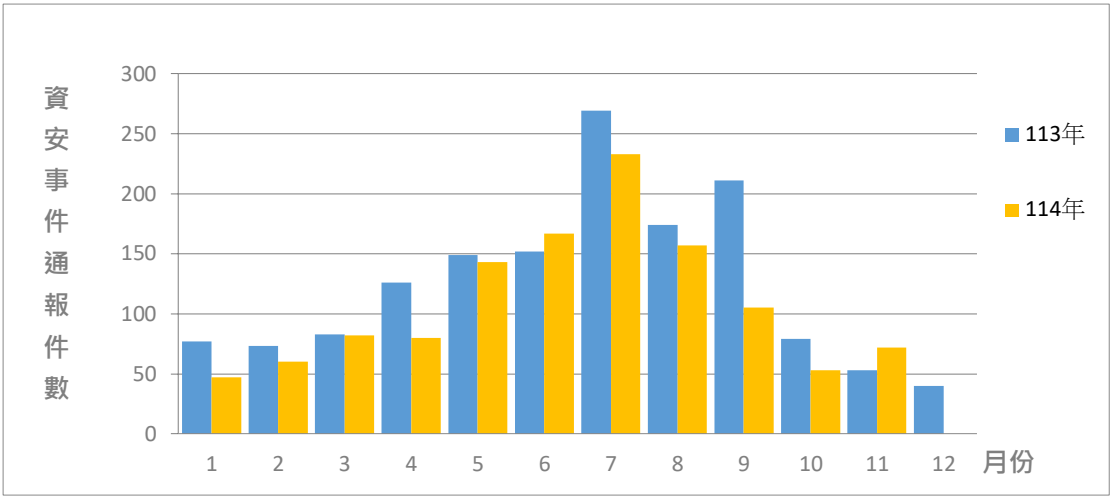

圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	壓縮程式 7-Zip 25.01(不含)以下版本 嚴重程度： CVSS 3.6 (CVE-2025-55188)	• 研究人員發現 7-Zip 存在連結追蹤(Link Following)漏洞(CVE-2025-55188) • 未經身分鑑別之本機端攻擊者可利用此漏洞寫入任意檔案。該漏洞目前已遭駭客利用。 • 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。
	WordPress 擴充程式/網頁主題	• 研究人員發現 WordPress 擴充程式與網頁主題存在 PHP 本機檔案包含(PHP Local

警訊	類別	內容說明
	存在 10 個高風險安全漏洞 嚴重程度： CVSS 9.8 (CVE-2025-67522、CVE-2025-67523、CVE-2025-67524、CVE-2025-67525、CVE-2025-67526、CVE-2025-67527、CVE-2025-67529、CVE-2025-67530、CVE-2025-67531 及 CVE-2025-67532)	File Inclusion) 漏洞 (CVE-2025-67522、CVE-2025-67523、CVE-2025-67524、CVE-2025-67525、CVE-2025-67526、CVE-2025-67527、CVE-2025-67529、CVE-2025-67530、CVE-2025-67531 及 CVE-2025-67532)。 • 未經身分鑑別之遠端攻擊者可利用此漏洞，誘使伺服器端 PHP 程式載入本機非預期檔案，並於伺服器端執行任意程式碼，請儘速確認版本並進行修補。 • 相關連結: https://www.cve.org/CVERecord?id=CVE-2025-67522 https://www.cve.org/CVERecord?id=CVE-2025-67523 https://www.cve.org/CVERecord?id=CVE-2025-67524 https://www.cve.org/CVERecord?id=CVE-2025-67525 https://www.cve.org/CVERecord?id=CVE-2025-67526 https://www.cve.org/CVERecord?id=CVE-2025-67527 https://www.cve.org/CVERecord?id=CVE-2025-67529 https://www.cve.org/CVERecord?id=CVE-2025-67530 https://www.cve.org/CVERecord?id=CVE-2025-67531 https://www.cve.org/CVERecord?id=CVE-2025-67532

警訊	類別	內容說明
	遠端設備管理軟體 研華科技 WISE-DeviceOn Server 嚴重程度：CVSS 9.8 (CVE-2025-34256)	• 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)。 • 研究人員發現研華科技 WISE-DeviceOn Server 存在使用硬刻之加密金鑰(Use of Hard-coded Cryptographic Key)漏洞(CVE-2025-34256)， • 未經身分鑑別之遠端攻擊者可自行製作 token 以偽冒任意 DeviceOn 帳號，進而取得完整控制權。 • 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	作業系統 Cisco AsyncOS 嚴重程度：CVSS 10.0 (CVE-2025-20393)	• 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)。 • 研究人員發現 Cisco Secure Email Gateway (SEG)與 Secure Email and Web Manager (SEWM)所使用之 AsyncOS(Cisco 專用)作業系統存在不當輸入驗證(Improper Input Validation)漏洞(CVE-2025-20393)。 • 未經身分鑑別之遠端攻擊者可利用此漏洞以 root 權限於受影響設備底層作業系統執行任意指令。 • 官方已提供安全公告，請參考官方說明儘速確認並採取相關緩解措施。

警訊	類別	內容說明
	開源 JavaScript 函式庫 React Server Components 嚴重程度：CVSS 10.0 (CVE-2025-55182)	• 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 • 研究人員發現 React Server Components 在解析傳向 Server Function 端點的序列化資料時，存在安全漏洞(CVE-2025-55182)。 • 攻擊者可在無需身分驗證的情況下，透過發送特製的惡意負載，達成遠端程式碼執行。 • 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

➢ 美國 CISA 與 NSA 就中國「磚塊風暴」(BRICKSTORM) 惡意軟體發出警告

(資料來源：The Record)

12 月 4 日，美國 CISA、國家安全局 (NSA) 與加拿大網路安全中心 (CCS) 聯合發布一份關於「磚塊風暴」(BRICKSTORM) 惡意軟體的警告，該警告基於來自受害機構的樣本。「磚塊風暴」是一種複雜的後門惡意軟體，與中國政府支持的駭客組織有關，其攻擊目標是政府和 IT 產業的機構，並長期駐留於受害系統中。此惡意軟體主要影響 VMware vSphere 和 Windows 環境，可用於提取憑證和建立隱藏虛擬機器以進行隱藏存取。該惡意軟體具有自我監控功能，可在中斷時自動重新安裝或重新啟動。此外，該惡意軟體也被用於瀏覽、上傳、下載、建立、刪除和篡改檔案。在

一些樣本中，它被用於橫向移動，從而進一步入侵其他系統。CISA 官員拒絕明確說明聯邦機構是否受到「磚塊風暴」的影響。

➢ **美國國家標準與技術研究院 (NIST) 計畫建構人工智慧代理威脅與緩解分類體系**
(資料來源：Security Boulevard)

美國國家標準與技術研究院 (NIST) 正在開發一套人工智慧代理威脅與緩解分類體系，旨在應對人工智慧快速普及帶來日益增長的安全風險。該計畫在紐約人工智慧高峰會上宣布，旨在系統性識別和分類人工智慧代理特有的攻擊面，從而加強現有的網路安全框架。目前，這些框架不足以保護企業級人工智慧應用。 NIST 強調了這項工作的緊迫性，並引用安全研究人員在測試中能夠從大型語言模型 (LLM) 中提取敏感資料的成功案例。隨著各組織機構嘗試使用日益自主的人工智慧代理，此分類體系將為管理新型數位身分和權限，以及緩解諸如影子人工智慧和即時注入攻擊等風險提供重要的指導。

五、 資安宣導資訊

(一) 政府組態基準（GCB）發展資訊

政府組態基準(Government Configuration Baseline，簡稱 GCB)目的在於規範資通訊設備(如個人電腦、伺服器主機及網通設備等)的一致性安全設定(如密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之風險。

114 年 GCB 發展項目計有 Apple macOS 15、Safari、AWS 基礎環境及 Fortinet Fortigate 等 4 項，另 115 年預告版說明文件與「115 年政府組態基準 GCB_意見徵詢表 v1.0」已公告於 GCB 專區(https://s.moda.gov.tw/2mtunS9EnATA)，歡迎下載並於 115 年 6 月

30 日前填妥意見徵詢表電郵（GCBService@nics.nat.gov.tw）提供調整與修訂建議。如有相關問題，亦可洽國家資通安全研究院檢測防禦中心，聯絡電話(02) 2739-1000 分機 23。

(二) 請資通安全責任等級 C 級以上機關（構）踴躍提報 115 年公務人員高等三級考試「資通安全類科」職缺

為紓解各機關資安業務人力需求，自 113 年起於公務人員高等考試三級考試增設「資通安全類科」，招募具資安專業能力之新進公務人員，以提供政府長期穩定資安人力來源。請依行政院人事行政總處公告作業時程，提報相關職缺，以進用資安專才人員，提升機關資安防護能量。

六、近期重要資安會議及活動

日期	活動/會議	對象
1 月 9 日	資安技能金盾獎決賽暨頒獎典禮	參加資安技能金盾獎之國高中、大專院校學生
1 月 16、17	資安防護實戰菁英返校日	歷年(110-113 年)資安菁英班結訓學員