國家資通安全研究院
National Institute of Cyber Security

資安週報

Cyber Security Weekly Newsletter

事件通報
網站下載功能於建置、改版或調整時 不宜忽視權限控管與檔案路徑設定

聯防監控
防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕
Web服務系統攻擊趨勢增加

重大漏洞
Oracle、Palo Alto Networks、Ivanti及Microsoft等產品存在高風險漏洞 應儘速落實更新與修補

外部曝險分析
TLS憑證與弱加密協定為本期主要風險增加來源

實兵演練
實兵演練揭露驗證機制未完善 避免僅於單一系統進行修補

網路巡查高風險詐騙
詐騙話術標榜「台灣」與各健康誘因 提高可信度引導私訊付款

焦點文章
115年上半年產業資安情資分享與趨勢重點

2026.06.11
048

資安儀表板

事件通報、聯防監控、蜜罐誘捕、重大漏洞、外部曝險分析及實兵演練等六類量化指標

■事件通報

近一週公務機關資安事件通報之類型與數量，同時包含民營機構依規定揭露重大資通安全訊息

網站下載功能於建置、改版或調整時 不宜忽視權限控管與檔案路徑設定

本週總計接獲17件公務機關與特定非公務機關事件通報，詳見圖1，公務機關非法入侵事件中以異常連線占多數，詳見圖2。本週有機關檢視日誌發現，可疑IP掃描探測官網目錄，並嘗試存取網站內檔案。經查，部分檔案只要取得連結即可直接下載，無須登入網站或經權限驗證，機關後續已調整下載檔案權限，以限制未授權存取。

此類情形多與網站下載機制或目錄權限設定疏漏有關，致非公開檔案於連結遭取得後，仍可能在未登入或未經權限驗證情況下被直接下載。建議可從功能授權、檔案路徑、存取測試及資料存放等面向檢視：確認各項功能之開放條件與實際需求一致，留意非公開檔案是否位於可直接存取之位置或存在僅憑連結即可下載之情形，並於上線前測試未登入、直接輸入連結及不同權限帳號之存取結果；對於機敏資料、備份檔或暫存檔案，則不宜存放於網站可公開存取路徑；另應持續留意目錄掃描、異常下載頻率及可疑來源IP等行為，以利及早發現風險。

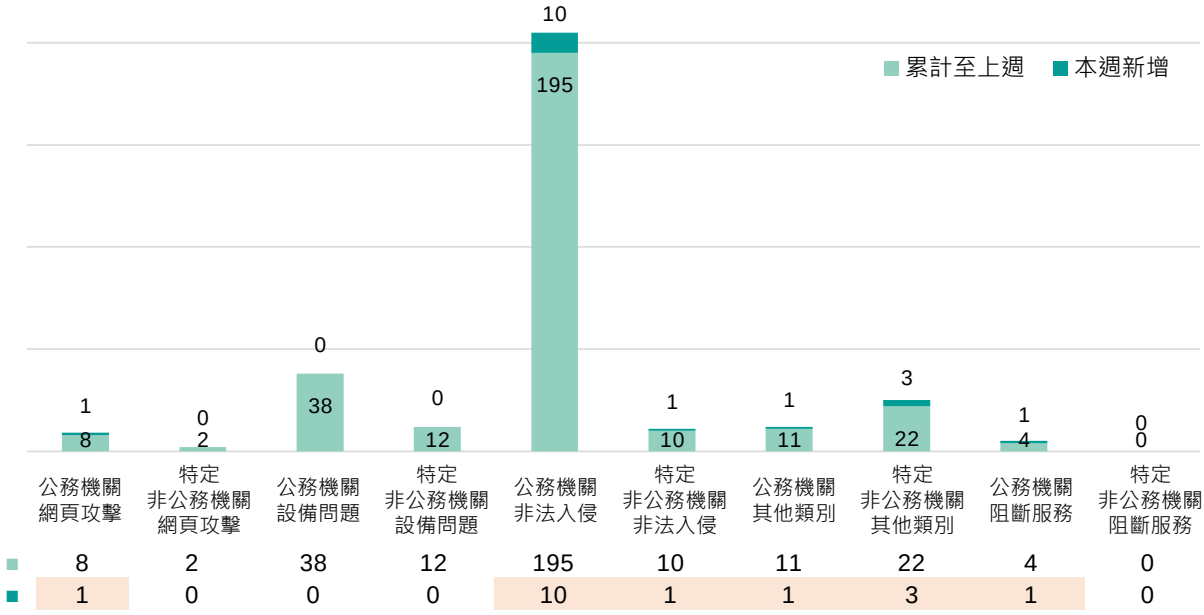

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

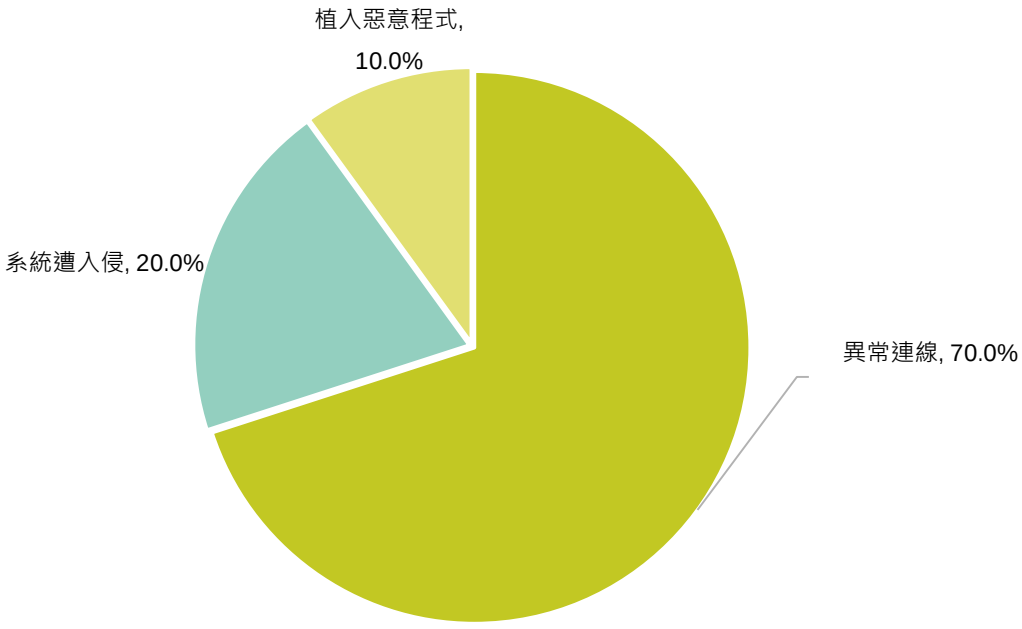

圖2 | 本週公務機關非法入侵事件類型占比

防護建議 **除修補漏洞外，應：**

以攻擊為出發評估潛在風險	針對潛在風險執行相應改善
➢ 官網目錄遭可疑IP掃描探測，易暴露敏感目錄結構與未公開路徑 ➢ 下載機制缺乏驗證，攻擊者取得連結即可直接下載非公開機敏檔案	➢ 調整下載權限與落實功能授權，限制非公開檔案須經身分驗證與授權方可存取 ➢ 落實上線前安全測試，驗證未登入及不同權限帳號之阻斷存取結果 ➢ 隔離機敏與備份檔案，嚴禁存放於網站可直接公開存取的網頁路徑 ➢ 持續監控目錄掃描與異常下載，及時阻斷可疑來源IP以利及早防範

1間民間企業揭露重大資安訊息

本週1家民間企業發布重大訊息，產業類別為其他電子業，詳見表1。

表1 | 本週民間企業重大資安訊息彙整

公司名稱	發布時間	事件說明
巨路國際股份有限公司	115年6月2日	巨路公司偵測部分資訊系統遭駭客網路攻擊時，已立即啟動資安防禦與通報機制，並與外部資安專家協同處理。 目前正對相關系統進行全面性的資安掃描與檢測，於確保資訊安全無虞後，利用日常備份資料陸續復原系統運作。經評估對公司營運無重大影響，亦未發現個資或機密資料外洩之情事，後續將持續強化網路與資訊安全架構，並擴大資安防禦措施，以提升整體資安防護能力。

■聯防監控

近一週以MITRE ATT&CK Matrix 分析攻擊者行為，提醒公務機關留意攻擊趨勢變化，是否由初期之偵測刺探進入影響層面更大竊取資料與破壞資通系統

防禦迴避高居首位 偵測刺探仍具威脅

本週政府領域資安聯防監控參考MITRE ATT&CK Matrix分析TTP戰術框架分布顯示，本週趨勢相較上週無顯著差異，詳見圖3。「防禦迴避」為最常見攻擊手法，占比15.1%，攻擊者通常會透過關閉或刪除指令紀錄，並利用合法的系統工具間接執行惡意命令，以達到規避監控的目的。因應此類威脅，建議導入端點防護措施，加強指令紀錄的稽核能力，限制高風險工具的濫用，並強化特權帳號的管理，以避免攻擊者繞過偵測並消除其行為痕跡。

「偵測刺探」事件本週占比為14.5%，為本週占比次高的攻擊階段，顯示攻擊者持續加強對目標環境的前期偵查與弱點探測行動。觀察到的主要手法包括主動式掃描、IP 區段掃描、以及漏洞掃描。攻擊者透過自動化工具對大範圍網段進行探測，以識別對外服務、開放埠與系統類型，並進一步針對潛在弱點進行漏洞評估，尋找可利用的攻擊入口。此類行為通常呈現由廣泛掃描逐步聚焦的特徵，顯示其攻擊流程具備階段性與目標導向。由於此階段多發生於攻擊初期，若未及時偵測，將提高後續入侵成功機率。建議加強對異常掃描流量的監控與分析，導入漏洞管理與修補機制，並結合威脅情資比對掃描來源，以提前掌握潛在攻擊準備行為。

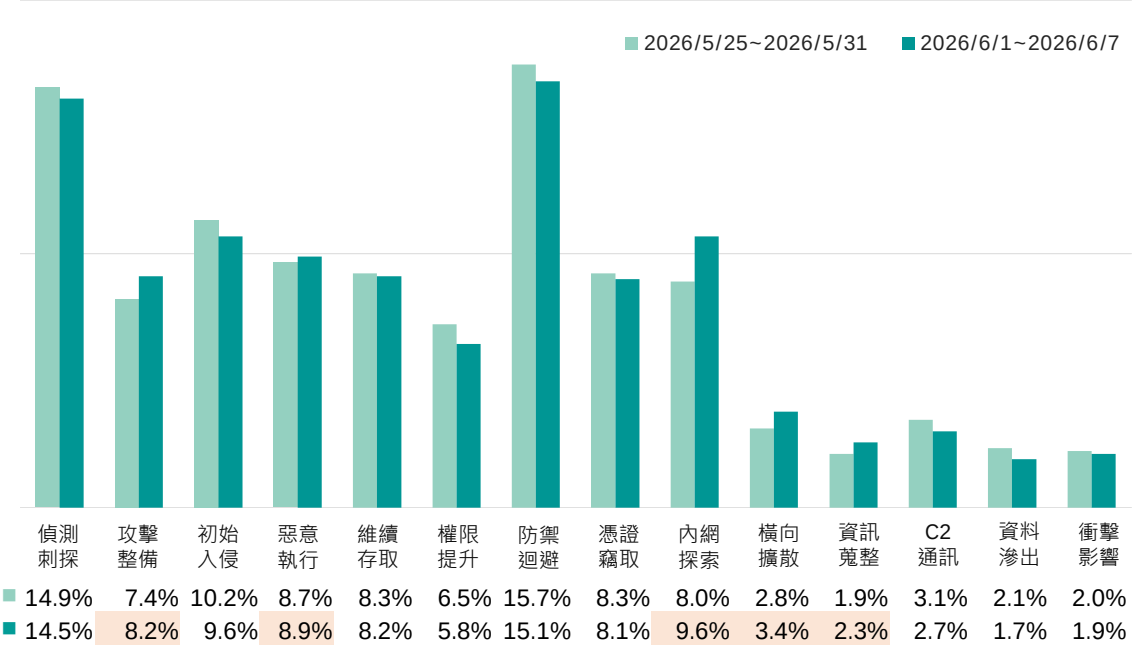

圖3 | 資安聯防監控攻擊階段統計

防護建議 **建議機關採取下列防護措施：**

防禦迴避（Defense Evasion）

- 啟用並保護系統與安全設備日誌，避免遭竄改或刪除
- 強化 PowerShell、CMD、WMI 等系統工具使用監控
- 導入 EDR/XDR 等端點偵測與回應機制
- 落實最小權限原則，限制高權限帳號使用
- 建立異常程序執行與權限提升行為告警機制
- 定期檢視特權帳號活動與系統設定變更紀錄

偵測刺探（Reconnaissance）

- 監控異常掃描流量與大量連線行為
- 建置 IDS/IPS偵測網路掃描及探測活動
- 定期執行弱點掃描與修補管理作業
- 限制非必要對外服務及開放連接埠
- 導入威脅情資比對，識別惡意掃描來源
- 建立網路流量基準，及早發現異常偵察行為
- 強化資產盤點，掌握對外暴露系統狀況

■蜜罐誘捕

近一週誘捕系統所捕捉到的攻擊樣態趨勢變化以及所利用的弱點趨勢

Web服務系統攻擊趨勢增加

本週透過部署於國內外之蜜罐系統觀測攻擊行為動態，相較於上週「網頁應用」服務攻擊占比68.19%、「遠端控制」服務攻擊占比28.82%，本週各類服務之平均偵測攻擊比例無明顯變化，結果顯示「網頁應用」服務仍為攻擊主軸，占比高達71.94%。「遠端控制」服務亦有24.43% 的誘捕比例，反映攻擊者仍積極針對公開遠端連線介面進行入侵行動。

網頁應用是最為常見之對外服務類型，若存在已知漏洞，將面臨高風險曝露情形，易成為攻擊者入侵與滲透重要管道，為優先防護之項目。本週網頁應用介面之誘捕狀況，詳見圖4。本週通用型Web介面占比最高，此類別為攻擊者廣泛的進行HTTP掃描與探測，顯示攻擊者企圖尋找可能存在之Web漏洞進行攻擊。

另Web服務系統類別包含各類以網頁為基礎的服務與應用，例如常見的網頁框架、應用程式伺服器、檔案傳輸與資料管理平台等，由於此類服務多建置於企業應用環境，且直接面向外部提供功能與資料交換，為僅次於通用型介面的攻擊目標。而Web服務系統比例上升主因為cPanel & WHM在登入流程中存在身份驗證繞過漏洞的CVE-2026-41940，遭攻擊次數上升導致。網通設備管理介面涵蓋路由器、防火牆等網通設備管理介面，以及智慧攝影機、NAS等物聯網設備管理介面，皆容易遭受攻擊者透過弱密碼、預設帳號或已知漏洞進行入侵。其他類型服務雖比例極小，但若涉及關鍵業務系統，仍需留意潛在風險。

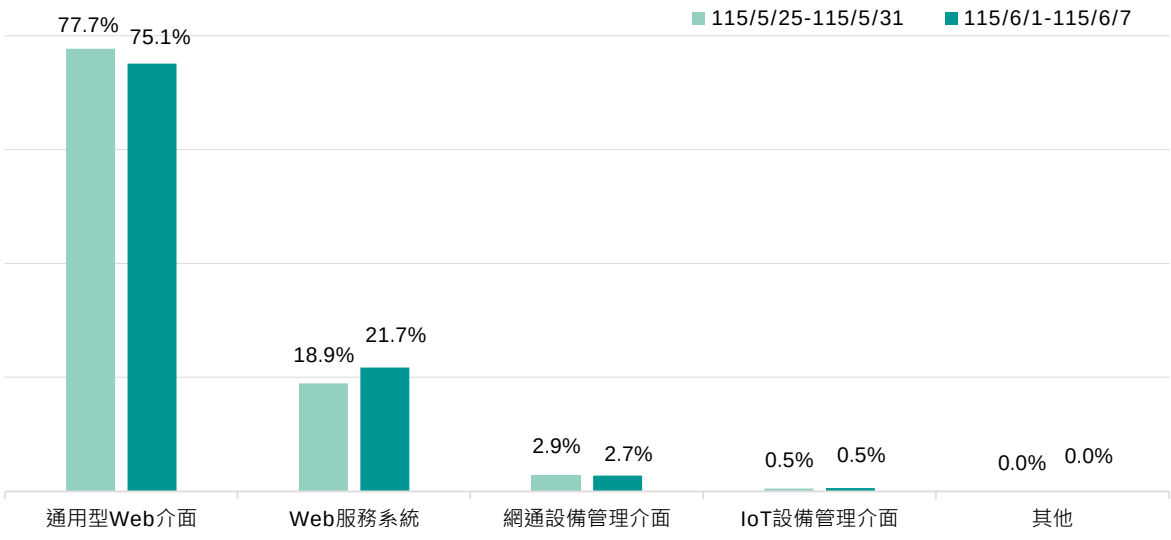

圖4 |本週網頁應用介面之誘捕攻擊比例統計

進一步解析國內外之蜜罐系統誘捕漏洞攻擊之情形，詳見表2。近2年揭露之攻擊漏洞，前5大攻擊以「網頁應用」服務之漏洞為主要入侵路徑，本週漏洞類型多集中於越界讀取漏洞、身分驗證繞過漏洞、跨站請求偽造、授權缺失漏洞及資訊外洩漏洞，攻擊目標涵蓋程式遞送控制器(ADC)、網站主機伺服器管理系統、多選下拉選單元件、企業級網路防火牆軟體及開放原始碼的後端伺服器框架。

防護建議

建議存在漏洞之設備應更新至最新版本軟體或韌體以修補漏洞；若原廠已無法提供更新支援，應考慮汰換存在漏洞之設備或軟體套件，如因故無法汰換，應採對應之漏洞緩解措施。

表2 | 本週前5大攻擊使用之近2年漏洞排行列表

排名			漏洞編號	受影響產品	CVSS 3.x Base Score
■	1	-	CVE-2025-5777[1]	Citrix NetScaler ADC	7.5
■	2	⬆2	CVE-2026-41940[2]	cPanel & WHM	9.8
■	3	⬇1	CVE-2025-47204[3]	Bootstrap Multiselect	6.1
■	4	⬇1	CVE-2025-20362[4]	Cisco Secure ASA & FTD	6.5
■	5	⬆new	CVE-2025-53364[5]	Parse Server	5.3

類型 ■ 越界讀取漏洞 ■ 身分驗證繞過漏洞 ■ 跨站請求偽造
■ 授權缺失漏洞 ■ 資訊外洩漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
3. https://nvd.nist.gov/vuln/detail/CVE-2025-47204
4. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
5. https://nvd.nist.gov/vuln/detail/CVE-2025-53364

■重大漏洞

近一週本院研究人員發現以下重大漏洞資訊，建議組織內部進行檢查與修補

Oracle、Palo Alto Networks、Ivanti及Microsoft等產品存在高風險漏洞 應儘速落實更新與修補

- Oracle釋出115年5月份安全性更新，共修補包含Oracle Database Server與Oracle E-Business Suite等共35個漏洞，其中有16個漏洞屬於高風險[1]。
- Palo Alto Networks PAN-OS軟體之GlobalProtect portal與gateway存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-0257[2])，未經身分鑑別之遠端攻擊者可利用該漏洞繞過身分鑑別，進而建立未經授權之VPN連線。
- Ivanti Neurons for ITSM存在不當存取控制(Improper Access Control)漏洞(CVE-2026-9614[3])，已取得一般權限之遠端攻擊者可繞過權限驗證機制取得管理員存取權限。
- Microsoft SharePoint存在不安全之反序列化(Insecure Deserialization)漏洞(CVE-2026-45659[4])，已取得一般權限之遠端攻擊者可透過對未受信任之資料進行反序列化，進而執行任意程式碼。

1. https://www.oracle.com/security-alerts/cspumay2026.html
2. https://nvd.nist.gov/vuln/detail/CVE-2026-0257
3. https://nvd.nist.gov/vuln/detail/CVE-2026-9614
4. https://nvd.nist.gov/vuln/detail/CVE-2026-45659

■外部曝險分析

經由外部檢測政府機關資通安全狀況，例如使用EASM工具或實兵演練，及早發現曝露於外部之風險

TLS憑證與弱加密協定為本期主要風險增加來源

本次針對曝險程度較高之93個A、B級關鍵基礎設施(CI)進行EASM資安曝險檢測，前10大風險項目共計2,788項。其中，「元件高風險漏洞」以915項居首，「過時或弱加密協定」以794項次之，「TLS憑證不受信任」以594項位居第三，詳見圖5。前三項合計2,303項，占前10大風險項目總數約82.6%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密通訊及憑證管理等議題。相較上期2,393項，整體風險數量增加395項，增幅約16.5%。

進一步分析重大風險變化情形，「元件高風險漏洞」由912項微增至915項，增加3項，增幅約0.3%，變化不大；「TLS憑證不受信任」由393項大幅增至594項，增加201項，增幅約51.1%；「過時或弱加密協定」由615項大幅增至794項，增加179項，增幅約29.1%；「CSP設定不當」由243項微增至245項，增加2項，增幅約0.8%，變化不大；「未部署WAF」則由103項降至95項，減少8項，降幅約7.8%。整體而言，外部曝險風險增加主要集中於憑證管理及加密通訊相關議題，網站應用層防護與安全設定仍須持續強化。

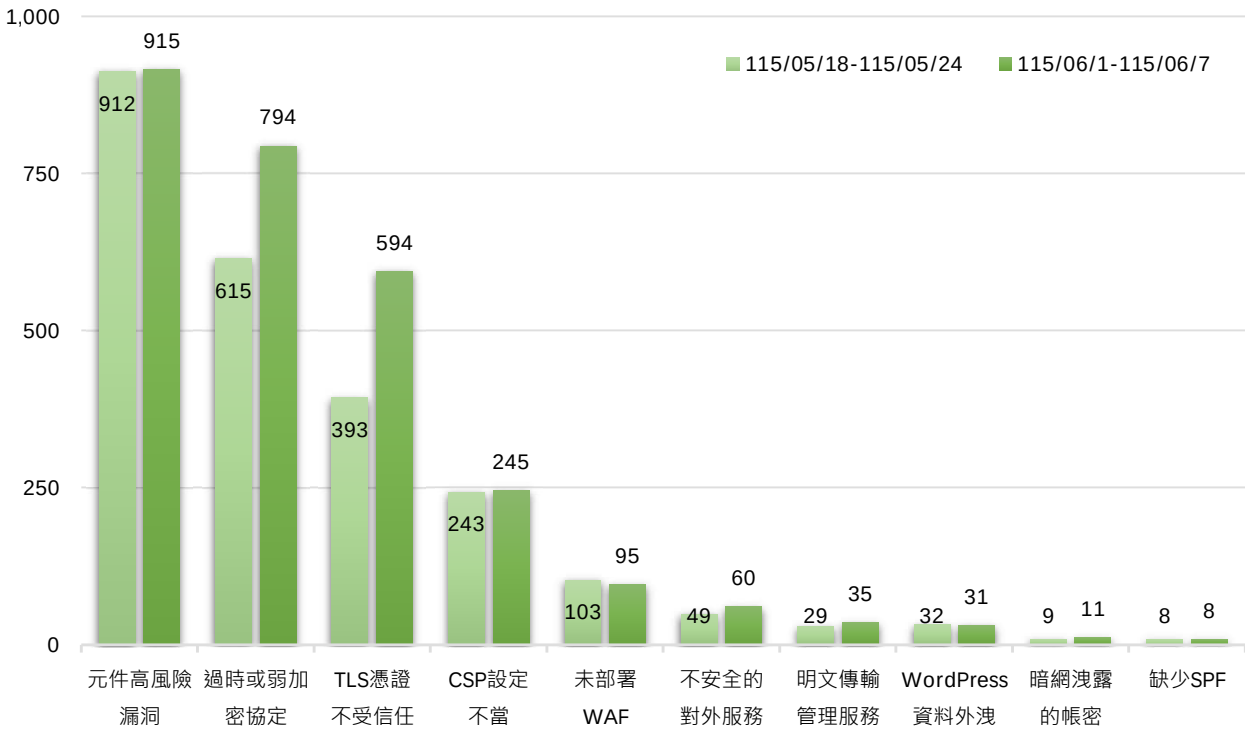

圖5 | EASM檢測結果統計(前10大風險)

防護建議

建議機關或關鍵基礎設施採取下列防護措施	建議機關或關鍵基礎設施採取下列管理措施
➢ 定期更新憑證，全面啟用TLS1.2以上版本協定，並停用未加密或舊版協定 ➢ 儘速修補已知漏洞，並淘汰已無維護之軟體版本 ➢ 部署網站應用程式防火牆(WAF)，並導入內容安全政策(CSP)等網站安全標頭，以降低XSS攻擊與惡意存取風險 ➢ 關閉不必要之對外服務，並定期盤點已停用站台、主機與應用服務是否已確實完成下線，避免因資產未完全下線而持續對外曝露；如確有遠端管理需求，應嚴格限制來源IP，並採用加密通道(如SSH)	➢ 定期盤點並更換外洩帳號憑證，搭配多因素驗證(MFA)，以強化存取安全 ➢ 建立弱點修補與驗證機制，確保風險持續改善 ➢ 強化資安教育訓練，提升系統維運人員對憑證管理、加密配置及服務設定之安全意識

■實兵演練

實兵演練係模擬真實攻擊情境，檢驗資通系統弱點、防護能力及應變機制，以提升整體資安防禦韌性

實兵演練揭露驗證機制未完善 避免僅於單一系統進行修補

本年資通系統實兵演練針對政府機關與關鍵基礎設施提供者，於擇定時間進行演練，至6/5止已累計130筆攻擊紀錄，本週新增弱點數量共57筆，分別為「驗證機制失效」27筆、「注入攻擊」7筆、「無效的存取控管」7筆、「軟體供應鏈失效」7筆、「加密機制失效」5筆、「不安全的組態設定」2筆、「Google Hacking駭侵手法」1筆及「不安全設計」1筆，詳見圖6。

本週演練發現「驗證機制失效」共計27筆，與上週發現之密碼強度不足及驗證機制未完善等問題雷同，係因不同機關使用同一廠商所開發之系統，尚未全面修補，導致攻擊者得以沿用既有手法持續觸發相同弱點並進行未經授權存取。另本週發現部分系統於頁面顯示時已對姓名與身分證字號等敏感資訊進行遮罩處理，惟攻擊者透過瀏覽器開發者工具或攔截封包分析系統回應內容後，仍可取得完整個資。

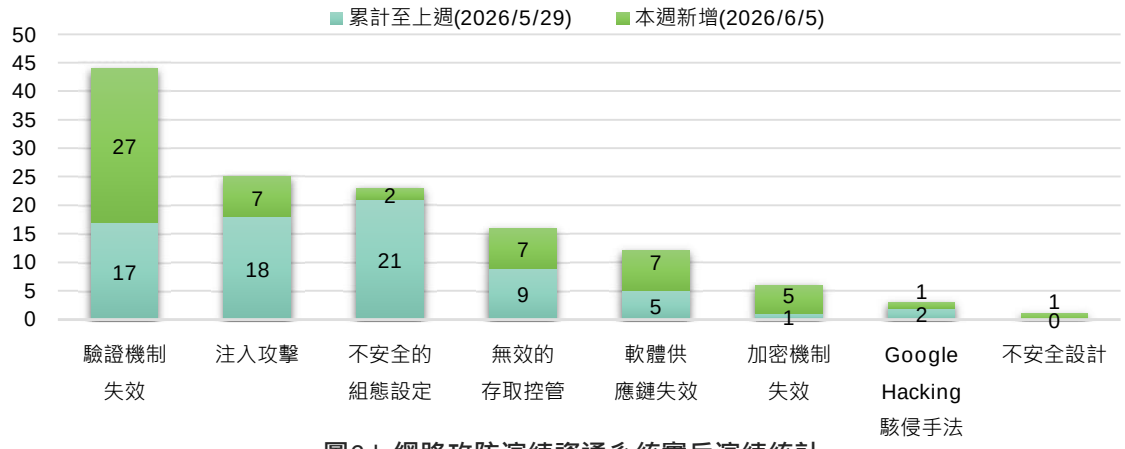

圖6 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 機關應全面檢視系統帳號管理與身分驗證機制，加強密碼強度政策，避免僅於單一系統進行修補，並針對相同架構或同廠商開發之系統進行一致性檢查，以降低類似弱點重複發生之風險
- 建議系統於後端完成資料遮罩或去識別化後再傳送至前端，避免將完整個資暴露於系統回應內容中；同時應依最小揭露原則提供資料，並定期檢視系統回應內容是否包含非必要之敏感資訊，降低個資外洩風險

■網路巡查高風險詐騙

追蹤詐騙訊息與手法演變，掌握政府機關實施之打詐政策與機制，是否達成其控制目標

詐騙話術標榜「台灣」與各健康誘因 提高可信度引導私訊付款

本週高風險詐騙關鍵字分析

本週高風險詐騙訊息最明顯的特徵，是「私訊」成為主要導流入口，並常與「台灣」、「問題」、「推薦」、「健康」、「免費」、「優惠」等高頻字眼共同出現。從廣告內容觀察，詐騙訊息常先用商品、健康、貸款、工作或命理服務吸引民眾注意，再透過「歡迎私訊」、「加 LINE 了解」、「留言後私訊教學」、「點擊下方按鈕」等方式，把民眾從公開頁面導向私人對話、短網址或不明表單，進一步蒐集個資、財務資料或引導付款。

「私訊」成為主要收口：公開貼文只是入口，真正風險在後續對話

本週「私訊」為最高頻關鍵字，相關內容涵蓋中古車貸、果樹苗販售、護眼產品、在家工作、法會報名等多種情境。常見話術包括「歡迎私訊」、「私訊了解名額有限」、「留言血壓我私訊你」、「加 LINE 下訂有折價」等，顯示詐騙訊息常先以廣告建立興趣，再把民眾導入私下聯繫。提醒民眾，凡商品價格、貸款條件、工作內容、報名方式或付款資訊必須透過私訊、LINE 或表單取得者，均應提高警覺；進入私人通訊管道後，對方可能要求提供個資、身分證件、銀行帳戶、信用卡或財務資料，也較容易避開平台交易保障及檢舉機制。

用「台灣」包裝在地可信度，降低民眾戒心

本週「台灣」出現次數高，常被用來營造在地製造、在地熱銷或交易安全的印象。例如服飾廣告標榜「台灣女生瘋搶」、「台灣設計」、「台灣熱銷」；保健與護具內容則強調「全程台灣生產製造」、「台灣皮膚科推薦」、「台灣青草配方」等，讓民眾誤以為來源清楚、品質可靠。惟「台灣」、「安心」、「品質保證」等字眼本身不代表交易安全。若賣場僅提供短網址、私訊或 LINE 聯繫，且缺乏清楚公司資料、產品標示、退換貨規範或客服管道，仍可能涉及假賣場、假認證、誇大療效或付款後失聯風險。

從「健康問題」製造焦慮，再用快速見效推動購買

本週「問題」、「健康」、「血壓」、「血管」、「糖尿病」、「中風」、「血栓」、「血糖高」、「阻塞」等關鍵字集中出現，顯示健康焦慮仍是重要話術。相關廣告常將高血壓、血糖、視力、腰椎、皮膚、男性體力、腎臟調養等議題包裝成急需處理的健康問題，再搭配「逆轉糖尿病」、「調節血壓血糖血脂」、「3天止癢」、「21天徹底治癒」、「無需手術」等說法，吸引民眾購買。

此類訊息常加入「醫師推薦」、「日本漢方」、「美國原裝進口」、「GMP 品質認證」、「專利配方」等背書字眼，提高可信度。提醒民眾，凡宣稱可快速改善疾病、逆轉病況、免治療或一次處理多種身體問題者，都應先查證產品合法性與醫療宣稱是否屬實。

「免費、優惠、零元」常是引導互動的第一步

本週「免費」、「優惠」、「了解」、「點擊」等字眼也具有高度風險意義。常見內容包含「一盒免費體驗」、「免費測算」、「死苗免費補發」、「0 元帶回家」、「零頭期」、「免費教學」、「在家接單」、「無經驗可」等，先讓民眾覺得成本低、門檻低、現在參與很划算。但後續可能轉為要求填寫表單、提供個資、加入 LINE、提供財力資料，或先支付訂金、手續費、運費、保證金。提醒民眾，凡以免費、零元、優惠、低利率或無經驗可作為吸引點，卻在後續要求提供個人資料、帳戶資料或先行付款者，均應暫停操作並查證來源。

圖7 | 詐騙關鍵字文字雲

本週防詐提醒

1. 「私訊」是本週最重要的風險訊號，凡廣告要求私訊、加 LINE、留言後才提供價格、連結、教學、貸款條件或報名方式者，應先查證商家身分與交易保障。
2. 看到「台灣熱銷」、「台灣設計」、「台灣製造」、「安心保證」等字眼，不代表一定可信，仍應確認公司資訊、產品標示、客服管道、退換貨規範及付款頁面是否安全。
3. 保健與身體相關商品若宣稱「逆轉糖尿病」、「調節血壓血糖」、「無需手術」、「3天見效」、「21天治癒」、「醫師推薦」、「日本漢方」等，應提高警覺，避免因健康焦慮購買來路不明商品。
4. 車貸、在家工作、免費測算、法會報名等內容若要求提供身分證件、銀行帳戶、財務資料，或先繳費、先匯款、先加入群組，應先暫停並查證合法性。
5. 凡出現短網址、不明賣場、資訊不完整，卻持續催促「限量補貨」、「名額有限」、「立即點擊」、「留言 +1」者，都應先停下來查證，不要在急迫感下完成付款或提供資料。

綜合觀察

綜合本週資料觀察，詐騙訊息多半先以「台灣」、「推薦」、「健康」、「必備」等字眼建立可信度與需求感，再用「免費」、「優惠」、「零元」、「限量」降低戒心，最後透過「私訊」、「LINE」、「點擊連結」完成導流。尤其本週健康焦慮與私訊導流結合明顯，從護眼、血壓、血糖、皮膚、腰椎到男性調理等內容，均可見以專業背書、快速見效及恐懼訴求包裝商品。提醒民眾，凡遇到不明連結、私訊交易、短網址、資訊不完整，或要求提供個資、信用卡、銀行資料及先付款才能取得商品或服務者，均應先行查證，以降低受騙風險，詳見圖7。

焦點文章

115年上半年產業資安情資分享與趨勢重點

從情資數據到攻擊趨勢：觀察產業資安風險的變化

根據TWCERT/CC上半年情資發送統計結果，駭侵事件仍為主要情資類型，漏洞情資次之，詳見圖8；若進一步分析事件內容，則以漏洞通報與產品安全事件占比最高，詳見圖9。從數據面觀察，攻擊者仍持續利用已知漏洞作為主要入侵手段，而產品安全問題則逐漸由單一系統風險擴大至軟體供應鏈與產品生命週期管理層面，近期情資內容亦呈現幾項值得關注的變化。

首先，攻擊活動與已知漏洞的關聯性持續提高，顯示攻擊者更傾向利用公開資訊快速發動攻擊，而非投入高成本開發新型攻擊技術。其次，產品安全相關事件增加，反映開源元件、第三方套件及軟體供應鏈已成為新的風險來源。最後，攻擊目標已逐漸由單一系統轉向開發流程及供應鏈信任關係，影響範圍也從單一組織擴大至上下游合作夥伴。

綜合上半年情資與公開事件觀察，可以發現正常網站遭植入外部腳本、產品安全治理要求，以及供應鏈攻擊向開發流程延伸，已成為產業值得關注的重點議題。

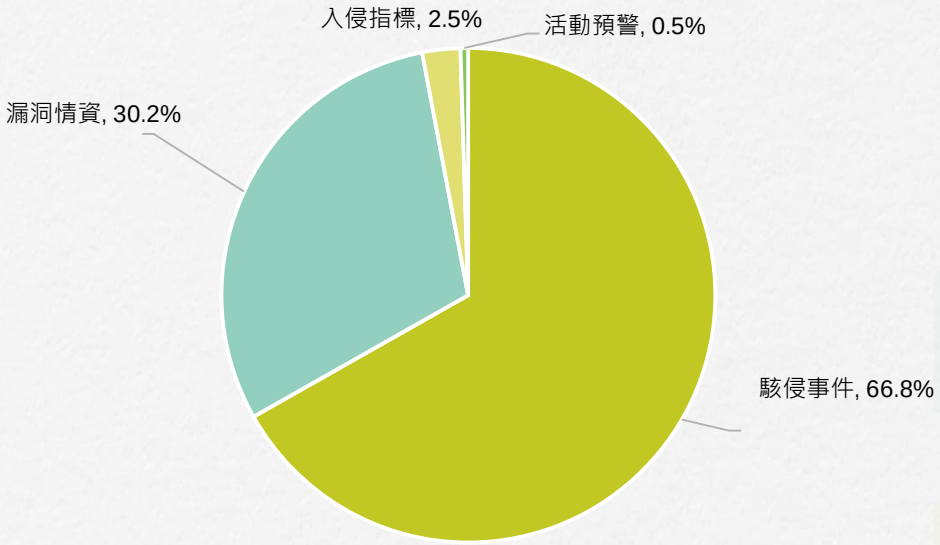

圖8 | TWCERT/CC情資發送類型

焦點文章

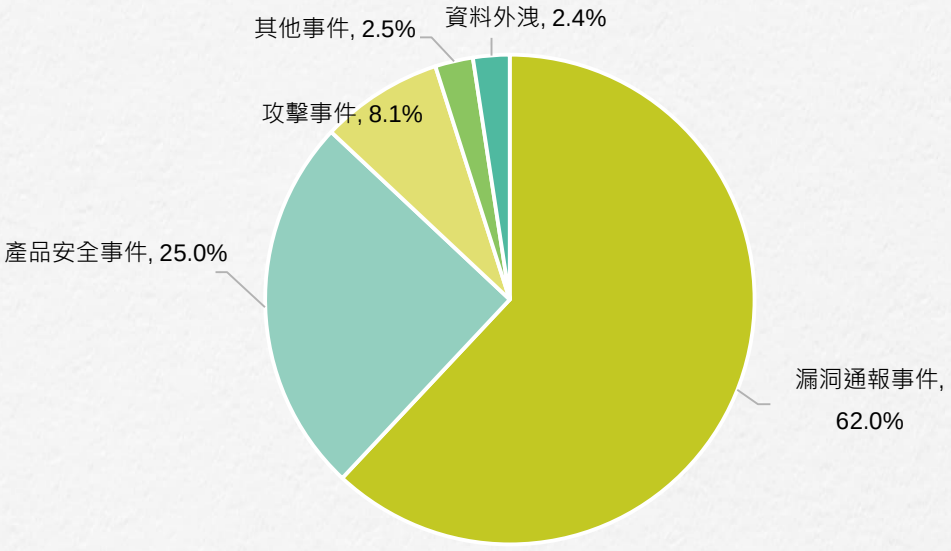

圖9 | TWCERT/CC通報資安事件類型

正常網站遭植入外部腳本，偽裝技術服務降低警覺

近期觀察到部分正常網站於使用者瀏覽時，會連線至不明外部網域 pki-tool.com，並嘗試載入類似 vue.js?v=ga 的 JavaScript 資源。該網域名稱含有「PKI」字樣，容易讓人誤以為與憑證或加密服務有關；然而，該外部資源並非網站可明確辨識的合法第三方服務，且其檔名與參數設計帶有偽裝成前端函式庫或網站分析腳本的特徵，顯示網站可能遭植入外部 JavaScript。

這類攻擊手法的重點不在於直接破壞網站，而是利用正常網站的可信度，在使用者瀏覽時載入外部 JavaScript，進一步進行導流、追蹤或載入後續惡意內容。值得注意的是，植入碼不一定存在於網站檔案中，也可能被寫入資料庫、CMS 後台設定、頁尾欄位、廣告碼區塊或公告內容。因此，若僅依賴檔案完整性檢查，可能無法發現異常。

建議網站維運單位定期盤點外連資源，檢查網站是否載入不明網域或可疑 <script> 標籤，並同步檢視資料庫內容、CMS 模板、外掛設定及近期異動紀錄，以降低網站被植入惡意 JavaScript 後長期未被發現的風險。

焦點文章

CRA 要求逐步明確化，SBOM 與 PSIRT 成為產品安全管理重點

隨著歐盟Cyber Resilience Act(CRA)要求逐步明確化，產品安全治理已成為全球聯網產品製造商必須面對的重要議題。其中，SBOM(Software Bill of Materials)與 PSIRT(Product Security Incident Response Team)是最近受關注的兩項要求，也逐漸成為企業檢視產品安全成熟度的重要指標。

近年重大漏洞事件發生後，許多企業面臨的問題並非缺乏修補能力，而是無法快速確認哪些產品、版本與客戶受到影響。例如，當開源元件或第三方函式庫爆出重大漏洞時，若企業平時未建立產品元件清單，就需要耗費大量時間重新盤點產品組成，進而影響修補、通知與對外溝通效率。因此，SBOM 可協助企業掌握產品內部元件組成，快速判斷漏洞影響範圍；PSIRT 則可建立漏洞接收、分析、修補、揭露及對外溝通流程，提升產品安全事件應變能力。

對資通訊產業與製造業而言，CRA 的影響不僅限於歐洲市場。隨著國際客戶對產品安全要求提高，企業是否具備 SBOM 管理能力、產品漏洞處理流程及安全治理機制，將逐漸成為供應鏈合作與市場競爭力的重要條件。

偽冒開發工具誘導下載，供應鏈攻擊延伸至開發流程

近期觀察到攻擊者偽冒 GitHub 專案、熱門開發工具下載頁或技術文件，透過搜尋引擎排名或廣告導流，誘導開發人員下載惡意程式。開發人員在尋找套件、範例程式或除錯工具時，若未仔細確認來源與維護者身分，可能將惡意程式安裝至工作環境。

一旦惡意程式進入開發環境，攻擊者可能竊取原始碼、API 金鑰、雲端憑證或 CI/CD 系統權限，甚至進一步影響產品建置與發布流程，使風險擴散至下游客戶。此類事件顯示，供應鏈攻擊已不只發生在軟體更新或第三方套件階段，開發人員日常使用的工具與下載來源，也可能成為攻擊入口。

焦點文章

建議企業建立開發工具與第三方套件來源驗證機制，要求開發人員從官方網站、可信套件庫或內部核准來源下載工具，並將原始碼平台、開發主機及 CI/CD 流程納入監控，以降低惡意工具進入開發流程的風險。

結語

綜觀上半年情資統計與公開事件，可以發現網站遭植入外部腳本、產品安全治理要求，以及供應鏈攻擊向開發流程延伸，看似分屬不同面向 ，但皆反映出相同趨勢：企業所面對的資安風險已逐漸由單一漏洞或單一系統問題，擴展至產品生命週期、開發流程與供應鏈信任關係等層面。

從正常網站遭植入可疑 JavaScript，到 SBOM 與 PSIRT 等產品安全治理要求逐步受到重視 ，再到開發流程成為供應鏈攻擊目標，均顯示資安防護已不再侷限於系統弱點修補，而是需要建立跨部門、跨流程且可持續運作的治理機制。 建議各單位於下半年持續強化漏洞管理、產品安全治理與供應鏈風險管理，並將網站安全、SBOM 管理、PSIRT 運作及開發環境保護納入整體資安策略規劃，以提升組織面對新型態威脅的韌性。

關鍵字：產品資安、軟體供應鏈安全 、網頁腳本攻擊

刊　　名　資安週報第 48 期
發 行 人　國家資通安全研究院　林盈達院長
主　　編　國家資通安全研究院　國際合作及資安治理中心
出 版 者　國家資通安全研究院
網　　址　www.nics.nat.gov.tw
訂閱網址　www.nics.nat.gov.tw/newsletter/
讀者信箱　www.nics.nat.gov.tw/mail2center/

國家資通安全研究院
National Institute of Cyber Security