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

資安週報

Cyber Security Weekly Newsletter

外部曝險分析
整體曝險持平 風險結構未見明顯變化

重大漏洞
Microsoft與VMware高風險漏洞應盡速修補

實兵演練
實兵演練揭露OTP驗證機制缺失 致未授權存取系統風險

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服務系統與網路防火牆為攻擊熱點

事件通報
網站轉寄功能遭濫用，可能提高詐騙訊息可信度 應強化防濫用機制及民眾查證意識

網路巡查高風險詐騙
投資導流升溫 產品服務型內容仍居主要風險

焦點文章
漏洞通報統計與趨勢

2026.08.06
056

資安儀表板

外部曝險分析、重大漏洞、實兵演練、聯防監控、蜜罐誘捕、事件通報及網路巡查高風險詐騙七類量化指標

■ 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

整體曝險持平 風險結構未見明顯變化

本次針對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2,919項。其中，「元件高風險漏洞」以940項居首，「過時或弱加密協定」840項次之，「TLS憑證不受信任」607項位居第三。前三項合計2,387項，占前10大風險項目總數約81.8%，顯示目前外部曝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2,917項，整體風險數量僅增加2項(約0.07%)，變化不大；前三項占比則由約81.9%微降至約81.8%，風險結構未見明顯變化，詳見圖1。

進一步分析主要風險項目變化情形，「元件高風險漏洞」仍為最大宗風險，數量由941項微降至940項，降幅約0.1%。其中，Apache HTTP Server相關弱點 (CVE-2024-38475)仍較為集中；本期Drupal核心相關弱點(CVE-2020-13671)與Archive_Tar相關弱點(CVE-2020-36193)已見減少，惟新增WordPress相關弱點(CVE-2026-60137、CVE-2026-63030)。「過時或弱加密協定」維持840項，無變化；「TLS憑證不受信任」由609項微降至607項，降幅約0.3%。另在網站防護設定方面，「CSP設定不當」由256項微降至251項，降幅約2.0%；「未部署WAF」由145項降至144項，降幅約0.7%。

整體而言，本期前10大風險項目變化不大，各受測單位仍需持續強化加密協定設定、憑證生命週期管理及網站安全防護措施。

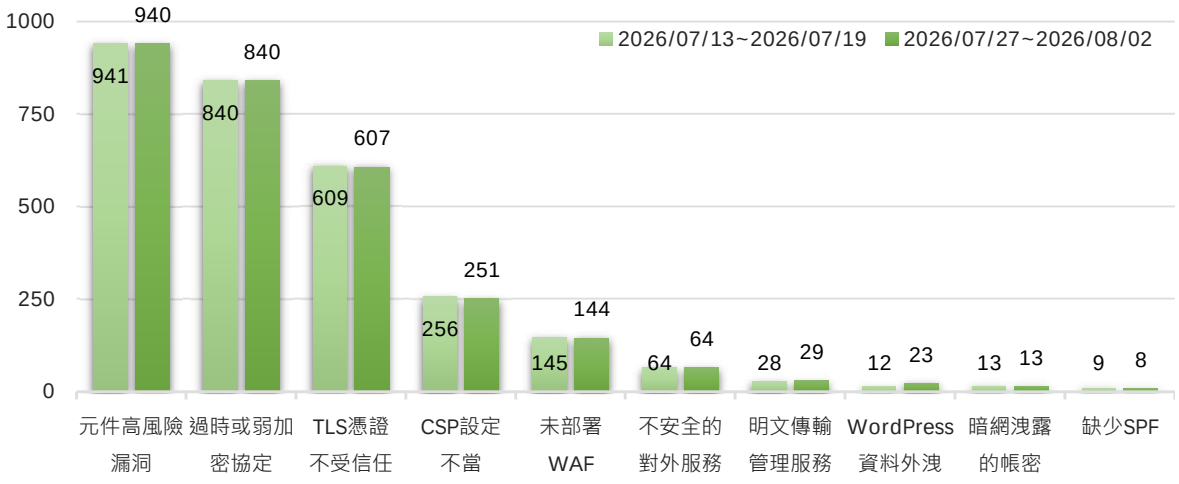

圖1 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施	建議受測單位採取下列管理措施
➢ 定期更新憑證，全面啟用TLS 1.2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、主機及應用服務是否已確實下線，避免資產未完全關閉而持續對外曝露；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生命週期管理、加密協定設定及對外服務管理之安全意識

■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

Microsoft與VMware高風險漏洞應盡速修補

- Microsoft Office SharePoint存在高風險漏洞(CVE-2026-50522)[1]，類型為不安全之反序列化(Insecure Deserialization)，未經身分鑑別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，該漏洞已遭駭客利用。

- VMware多項產品存在3項高風險安全漏洞(CVE-2026-47876、CVE-2026-59309及CVE-2026-59310)[2]，類型分別為越界寫入(Out-of-Bounds Write)、身分鑑別繞過(Authentication Bypass)及路徑遍歷(Path Traversal)。

  - ✓ CVE-2026-47876：已取得虛擬機器VMXNET3介面卡本機管理員權限之攻擊者，可於ESXi主機上執行任意程式碼。
  - ✓ CVE-2026-59309：已取得VMware vCenter網路存取權限之遠端攻擊者，可利用此漏洞於未經授權之情況下繞過身分鑑別並存取系統。
  - ✓ CVE-2026-59310：已取得VMware vCenter網路存取權限之遠端攻擊者，可利用此漏洞執行任意程式碼。

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522
2. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

■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OTP驗證機制缺失 致未授權存取系統風險

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7/31止已累計245筆攻擊紀錄，本週新增弱點數量共9筆，分別為「無效的存取控管」4筆、「注入攻擊」2筆、「軟體供應鏈失效」2筆及「不安全的組態設定」1筆，詳見圖2。

本週演練發現，高風險弱點為「驗證機制失效」。攻擊者於系統註冊流程中發現功能路徑，經瀏覽後取得明文帳號與密文密碼。攻擊者使用該帳號與任意密碼發起登入請求，並於驗證過程中攔截系統請求封包，將密碼欄位修改為發現之密文密碼後重新送出，進一步發現系統回應內容包含一次性驗證碼(One-Time Password, OTP)資訊。

經測試發現，該OTP驗證碼於多次驗證流程中均維持相同數值，未於使用後立即失效或重新產生，致攻擊者可重複利用該驗證資訊完成身分驗證並成功登入系統。登入後，攻擊者於系統管理功能中發現一組已停用之使用者帳號，嘗試重新啟用該帳號。經驗證該使用者帳號原處於停用狀態，重新啟用後即可正常登入系統，證實攻擊者取得之帳號具備系統管理者權限。

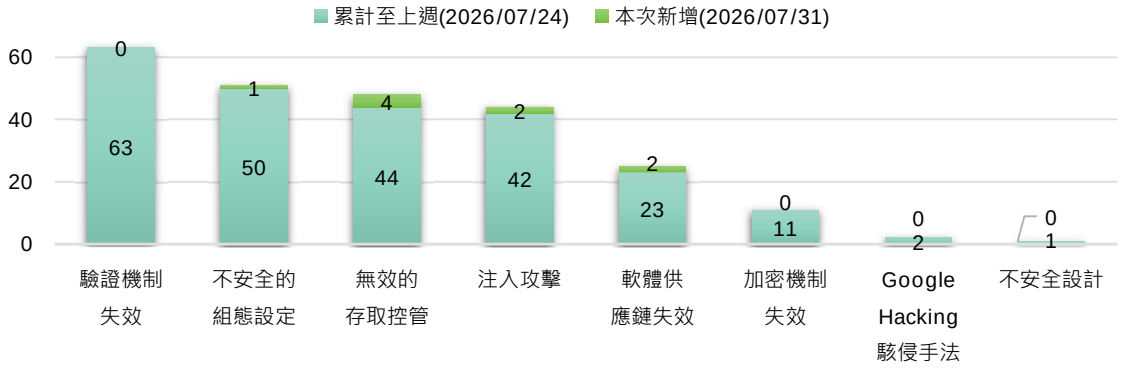

圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應強化身分驗證流程，OTP驗證碼應於每次驗證流程重新產生，並設定有效期限與單次使用機制，驗證完成或逾時後應立即失效，避免攻擊者重複利用相同驗證資訊繞過驗證機制
- 系統應於後端完整驗證帳號、密碼、OTP及Session等驗證資訊之關聯性，避免僅依賴前端傳送之參數或驗證資訊判定登入結果，降低驗證流程遭竄改或繞過之風險
- 系統不應於公開可存取之路徑或功能中暴露帳號資訊與密碼相關資訊，並應檢視系統目錄與檔案存取權限，避免未授權使用者取得敏感資訊

■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14.4%，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13.6%，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偵查與資訊蒐集活動，以提升後續攻擊行動的成功率。觀察到的主要手法包括主動式掃描、憑證資訊蒐集及IP 區段掃描。攻擊者透過自動化工具對外部網段與公開服務進行大規模探測，蒐集系統架構、開放埠與服務資訊，同時搜尋與帳號憑證相關的公開資料或外洩資訊，作為後續登入嘗試與目標鎖定的依據。部分活動呈現由廣泛掃描逐步聚焦特定系統與帳號的特徵，顯示其偵查行為具備明確的攻擊目標與規劃。

此類行為雖多屬攻擊前期準備階段，但其蒐集成果往往成為後續入侵與橫向移動的重要基礎。建議組織加強監控異常掃描流量與帳號探測行為，定期盤點對外暴露資產，並結合威脅情資分析可疑來源，以提前發現潛在攻擊準備活動並採取防禦措施。

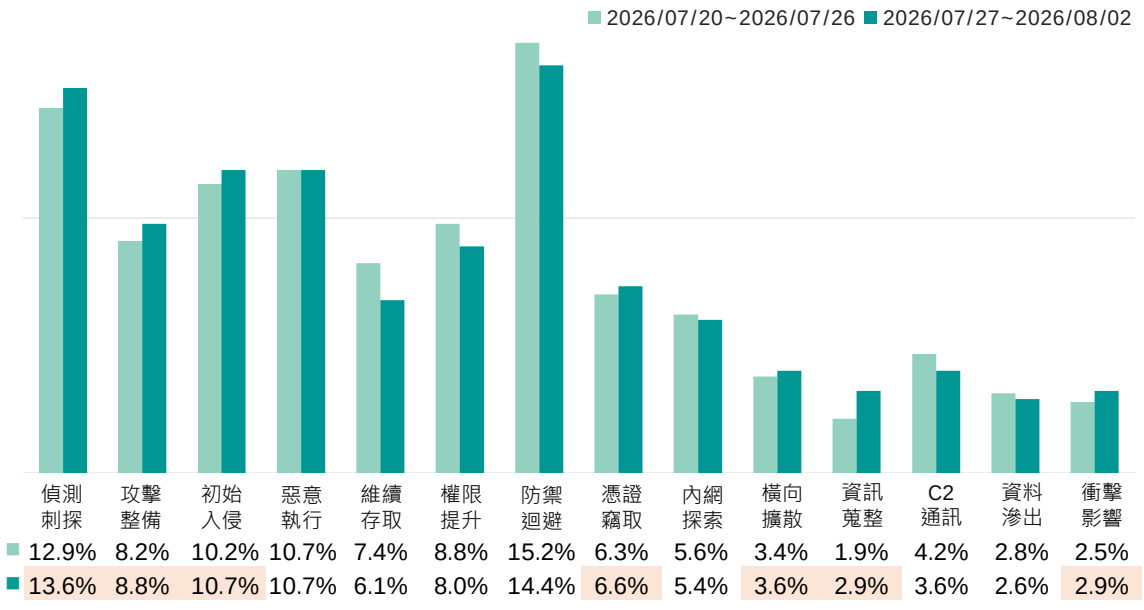

圖3 | 資安聯防監控攻擊階段統計

防護建議

建議機關採取下列防護措施

防禦迴避(Defense Evasion)

- 導入 EDR / 端點防護機制，提升惡意行為偵測能力
- 保留並定期稽核指令執行紀錄(如 PowerShell、Shell、CMD)
- 限制高風險系統工具(Living-off-the-Land Binaries, LOLBins)的使用權限
- 落實最小權限原則，加強特權帳號管理與多因素驗證(MFA)
- 建立日誌集中保存與防竄改機制，避免攻擊者刪除行為痕跡

偵測刺探(Reconnaissance)

- 監控異常掃描流量、連線探測及帳號枚舉行為
- 定期盤點並降低對外暴露資產，關閉不必要的服務與連接埠
- 持續修補公開服務漏洞，降低遭探測後利用的風險
- 結合威脅情資，封鎖已知惡意 IP、網段或掃描來源
- 強化帳號安全(MFA、強密碼、避免憑證外洩)，降低憑證蒐集成功率
- 定期檢視公開資訊(OSINT)，避免敏感系統或帳號資訊對外曝光

降低公開曝險、強化端點防護與持續監控，控制偵測刺探與防禦迴避攻擊

■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服務系統與網路防火牆為攻擊熱點

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73.06%、「遠端控制」服務攻擊占比23.38%，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73.72%。「遠端控制」服務亦有22.91% 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GeoServer程式碼注入漏洞之CVE-2024-36401，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。

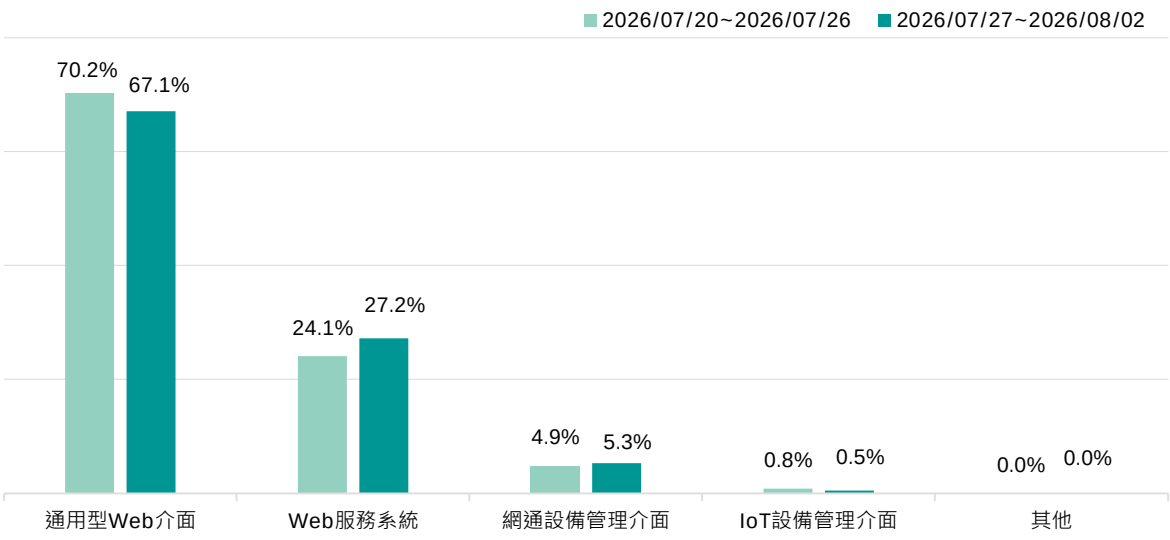

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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1。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授權缺失漏洞、路徑遍歷漏洞、資訊外洩漏洞、輸入驗證不當漏洞及跨站請求偽造，攻擊目標涵蓋企業級網路防火牆軟體、內容管理系統之網站優化外掛程式、開源後端伺服器框架、視覺化工作流程自動化工具及多選下拉選單元件。

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1 | 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-2025-20362[1]	Cisco Secure ASA & FTD	6.5
■	2	⬆3	CVE-2025-30567[2]	WordPress WP01	7.5
■	3	⬇1	CVE-2025-53364[3]	Parse Server	5.3
■	4	⬆new	CVE-2026-21858[4]	n8n	10
■	5	⬇2	CVE-2025-47204[3]	Bootstrap Multiselect	6.1

類型 ■ 授權缺失漏洞 ■ 路徑遍歷漏洞 ■ 資訊外洩漏洞
■ 輸入驗證不當漏洞 ■ 跨站請求偽造

1. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
2. https://nvd.nist.gov/vuln/detail/CVE-2025-30567
3. https://nvd.nist.gov/vuln/detail/CVE-2025-53364
4. https://nvd.nist.gov/vuln/detail/CVE-2026-21858
5. https://nvd.nist.gov/vuln/detail/CVE-2025-47204

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

網站轉寄功能遭濫用，可能提高詐騙訊息可信度 應強化防濫用機制及民眾查證意識

本週總計接獲18件公務機關與特定非公務機關事件通報，詳見圖5，公務機關非法入侵事件中以資料外洩占多數，主要係延續AI代理攻擊造成的資料外洩事件，詳見圖6。本週發現機關網站之「文章轉寄 / 分享」功能遭濫用，攻擊者於留言欄置入偽冒催繳、罰款等詐騙訊息及釣魚連結。由於郵件經官方網域寄出，易使收件者誤信，增加帳號及個資遭竊風險。

此類攻擊並非直接入侵郵件伺服器，而是利用網站既有功能及官方網域信譽，提高釣魚郵件的可信度，增加民眾帳號、個人資料或付款資訊遭竊風險。網站服務提供者應限制可輸入內容及外部連結，並導入驗證碼、寄送頻率限制、單一來源寄送上限及異常行為監控等機制。使用者收到以催繳、罰款或帳號異常為由的通知時，不宜僅因郵件來自官方網域即信任其內容，應避免直接點擊郵件內連結或輸入帳密、信用卡等資料，並改由機關官方網站、客服電話或既有服務入口查證通知真偽。

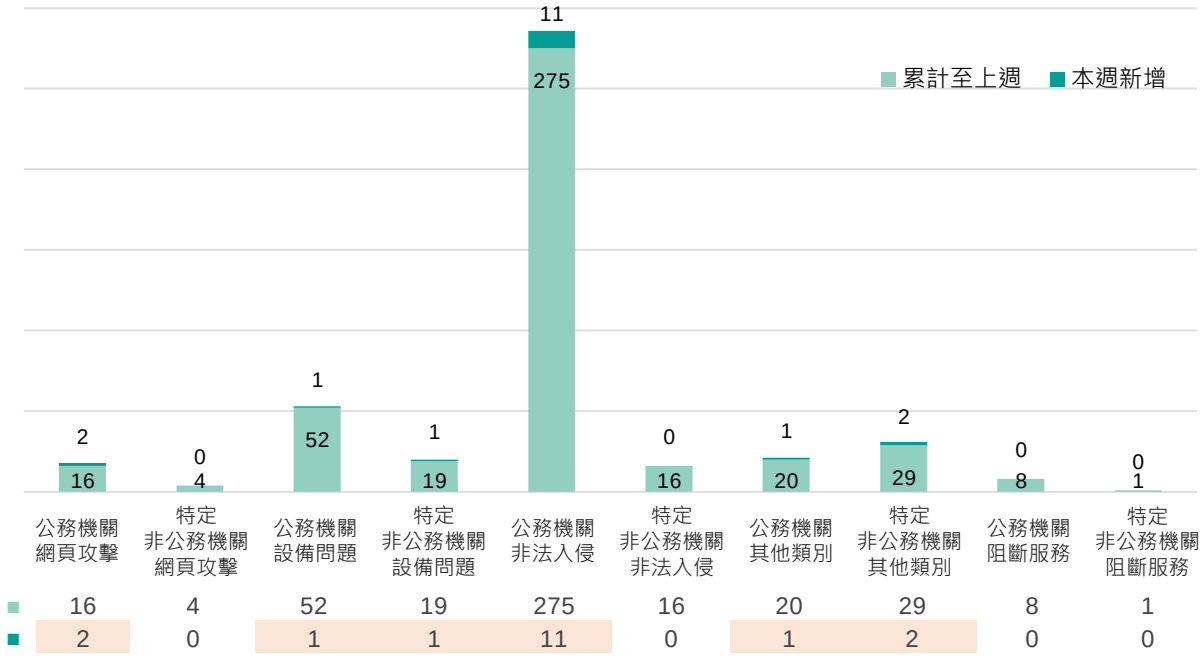

圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

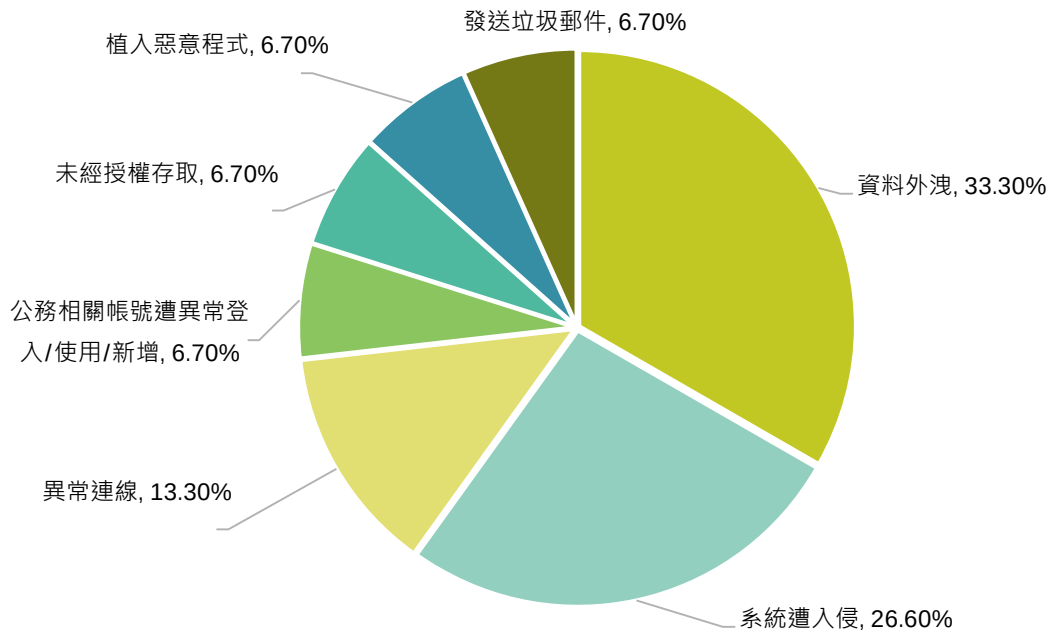

圖6 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者濫用網站分享功能寄送釣魚郵件，藉官方網域提升詐騙可信度 ➢ 民眾誤信官方網域郵件內容，導致帳號、個資或付款資訊遭竊取	➢ 限制文章分享內容與外部連結，避免遭植入釣魚網址或詐騙訊息 ➢ 導入驗證碼、寄送頻率及來源數量限制，防止大量濫發郵件 ➢ 建立異常寄送行為監控與告警機制，及早發現功能遭濫用情形 ➢ 定期檢視網站分享功能安全性，並宣導民眾透過官方管道查證通知真偽

2間民間企業揭露重大資安訊息

本週2家民間企業發布重大訊息，產業類別為居家生活業、電機機械業，詳見表2。

表2 | 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
萬達寵物事業股份有限公司	115年07月27日	萬達寵物因合作廠商資訊系統遭攻擊者入侵，疑似有個資外洩事件。萬達並無與合作廠商串接會員資料、信用卡號、銀行帳戶等敏感資訊，且已嚴正要求合作廠商技術團隊針對傳輸與系統環境進行最高規格的資安清查與漏洞修補，後續將持續監督其處理進度。
上銀科技股份有限公司	115年07月28日	上銀之義大利子公司部分資訊遭駭客攻擊時，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。目前針對相關系統進行全面資安掃描與監測，確保資訊安全無虞後，利用日常備份資料陸續恢復系統運作。 經初步評估對公司營運無重大影響，後續將持續強化網路與資訊基礎架構之安全防護機制及管理措施，以確保資訊系統穩定運作及資訊安全。

■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

投資導流升溫 產品服務型內容仍居主要風險

本週金融投資型占比由前週7.7%升至12.4%，增加4.7個百分點，為三類中增幅最大。相關話術主要運用「低門檻、免費體驗、即時資訊」降低民眾戒心，包括以免費模擬帳戶、低額開戶及即時黃金行情吸引投資，或以「領取最新資料」、「更新趨勢盤面」誘導點擊連結並加入LINE；另透過被動收入、避險操作及限時折扣包裝數位資產課程，詳見圖7。整體顯示，金融投資話術已由直接推薦標的，轉向模擬體驗、投資教學及社群導流等接觸方式。

身分冒充型占比由前週8.3%升至9.9%，增加1.6個百分點。相關內容著重運用專業機構、權威認證及名人形象建立信任，透過「醫學中心臨床實驗」、「國際權威期刊」、「防治指南」、「HACCP認證」及「明星同款」等說法，營造獲得第三方背書的印象。此類權威身分包裝降低民眾戒心，帶動身分冒充型內容占比回升。

產品服務型占比由前週84.0%降至77.7%，減少6.3個百分點，但仍占整體近八成。高風險商品涵蓋韓國服飾、中古車貸款、體重管理產品、草本保健品、血糖調理貼劑、防水噴劑及影音隨身碟等。常見手法包括境外品牌或技術背書、誇大健康功效、引用精確療效數字及限時優惠，再引導民眾透過私訊、LINE或陌生短網址交易。產品服務型占比雖然下降，仍是本週最主要的高風險類型。

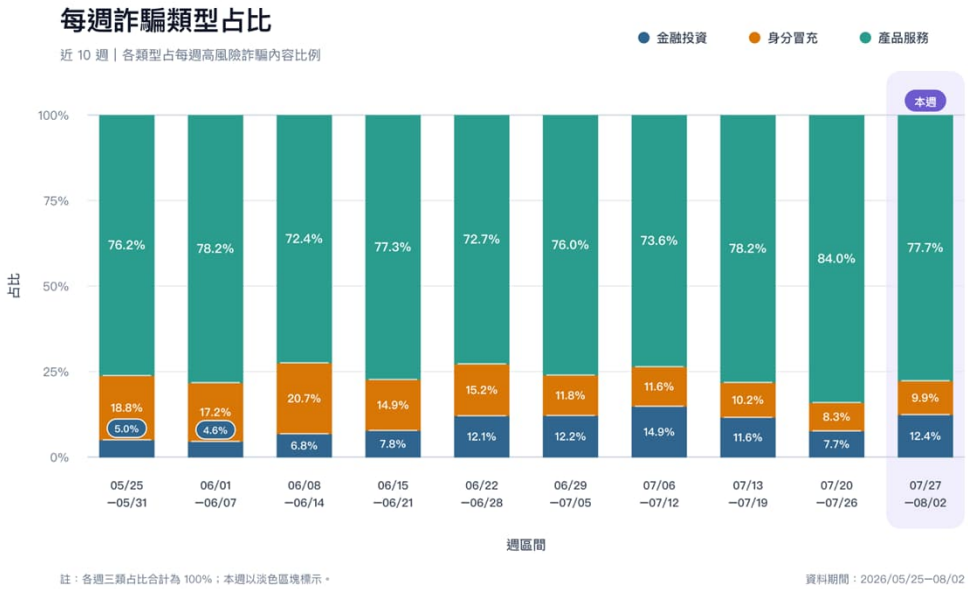

圖7 | 每週詐騙類型占比

「韓國」占比由前週3.88%升至5.41%，增加1.52個百分點，並升至本週首位，詳見圖8。前週主要出現在韓國偶像同款服飾，本週則擴及明星同款帽款及宣稱源自韓國的體重管理產品，顯示「韓國品牌」、「熱銷」及「明星同款」持續被用來營造流行形象與提高商品可信度。

體重管理產品是本週明顯升溫的話術主題。「控食錠」由2.93%升至5.15%，「飲食」由2.79%升至4.35%，「飽腹感」由2.60%升至4.03%，三項關鍵字共同反映體重管理產品的能見度提升。相關廣告宣稱產品可促進代謝、增加飽足感且無副作用，並以境外熱銷、安全認證及限時優惠等說法包裝，再透過留言、私訊或短網址引導購買。相關功效與認證屬廣告宣稱，民眾購買前應審慎查證。

保健醫療話術亦持續擴散。「輔助」由2.70%升至4.30%，主要反映血糖控制與穴位貼劑等訴求；「成分」由2.86%升至4.33%，呈現草本配方與天然原料的行銷特色；「控制」則由3.11%升至3.79%，顯示精確療效數字及人體臨床實驗等說法持續受到運用。相關廣告透過草本配方、精確療效數字、醫學機構及專業指南等元素包裝產品功效，已成為本週應重點關注的高風險話術。

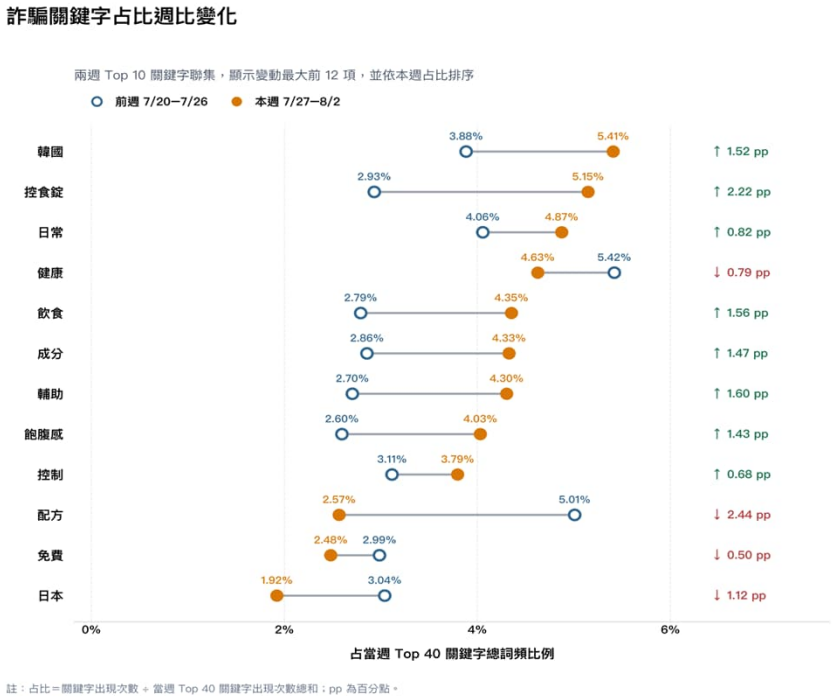

圖8 | 詐騙關鍵字占比週比變化

焦點文章

漏洞通報統計與趨勢

漏洞以輸入驗證居多，反映安全設計不足

115年第2季漏洞通報統計顯示，市售常見系統與軟體產品仍以「輸入驗證不足」為主要安全問題來源，同時於身分鑑別、授權機制及系統設定等面向，亦持續存在一定程度之資安風險。

為進一步了解漏洞分布情形，以下針對115年4月至6月期間之實際通報資料進行分析，TWCERT/CC TVN平台公告共計43筆漏洞，依其成因可進一步歸納為4大類別，包含輸入驗證、身分鑑別與授權、設定與環境及記憶體破壞，詳見表3。

表3 | 115/4~115/6 漏洞資料分析

漏洞類型		數量統計	
輸入驗證 (Input Validation)	Arbitrary File Upload	7	28
	SQL Injection	6	
	Insecure Direct Object Reference	3	
	OS Command Injection	3	
	Stored Cross-Site Scripting	3	
	Arbitrary File Deletion	2	
	Path Traversal	2	
	Arbitrary File Read	1	
	CRLF Injection	1	
身分鑑別與授權 (AuthN & AuthZ)	Missing Authentication	3	9
	Authentication Bypass	1	
	Brute-Force Protection Bypass	1	
	Improper Access Control	1	
	Missing Authorization	1	
	Privilege Escalation	1	
	Session Fixation	1	

漏洞類型		數量統計	
設定與環境 (Config & Env)	DLL Hijacking	1	5
	Exposed Dangerous Method or Function	1	
	Sensitive Data Exposure	1	
	Unquoted Service Path	1	
	Use of Hard-coded Credentials	1	
記憶體破壞 (Memory Corruption)	Stack-based Buffer Overflow	1	1
總計		43	

AuthN=Authentication，身分鑑別
AuthZ=Authorization，授權

焦點文章

以下將依各類型漏洞之比例與影響，逐一說明其重點與防護建議：

一、輸入驗證為主要漏洞類型(占比65.1%)

本類型漏洞共28個，占總數超過六成，輸入驗證不足仍為多數應用系統最常見之漏洞成因。顯示外部輸入格式、內容及檔案仍須加強控管。最主要類型如下：

- 任意檔案上傳(Arbitrary File Upload)共7件，若未妥善檢查檔案內容與副檔名，可能導致攻擊者上傳後門程式，進而取得伺服器控制權，風險相對較高。
- SQL注入(SQL Injection)共6件，顯示資料庫操作相關參數未妥善控管，易遭攻擊者利用以存取敏感資訊或竄改資料庫內容。

防護建議：

- 應採用「預設拒絕」原則，採取白名單機制，明確限制輸入格式、長度、字元集合與允許值，僅允許符合預期格式之輸入資料與上傳檔案格式，防止任何非預期的輸入與檔案上傳。
- 資料庫存取建議採參數化查詢，避免直接拼接外部輸入，以降低SQL Injection風險。

二、身分管理機制不健全(占比20.9%)

本類型漏洞共9個，多肇因於系統功能設計未完整考量權限邊界，或驗證邏輯存在缺陷，顯示敏感功能的身分確認與權限檢查仍有不足，主要集中在缺乏身分鑑別(Missing Authentication)類型，另外包含繞過驗證(Authentication Bypass)、不當存取控制(Improper Access Control)及缺乏授權機制(Missing Authorization)等。

- 身分鑑別包含管理介面、API及內部功能，建議系統管理功能預設進行身分鑑別機制，並評估以RBAC方式控管不同角色存取權限，避免鑑別流程設計不佳，遭攻擊者透過不同面向繞過檢查存取特定功能。
- 建議進行伺服器端權限檢查，以免攻擊者竄改特定封包參數，藉此越過系統權限限制，存取其他使用者的檔案或進行其他操作。

防護建議：

- 落實最小權限原則，確保每個帳號僅有執行任務所需之最小權限，定期檢視角色與權限，並清理閒置帳號與不再需要的授權。

焦點文章

- 應採用「預設拒絕」原則，對各物件與操作檢查使用者權限，避免僅以可預測之識別碼做為資料存取依據。
- 所有敏感功能與API，應於伺服器端執行身分鑑別並逐項授權，勿直接信任前端傳入之角色或狀態。

三、設定與環境管理不當(占比11.6%)

本類型漏洞共5個，多與系統部署與設定管理不當有關，通常源於安全設定與管理機制未落實所致，包含使用硬刻之帳號通行碼、暴露機敏資料或檔案及前端執行伺服器端安全機制不足等，顯示憑證、資料保護及安全設定需建立一致安全基準。

防護建議：

- 嚴禁將金鑰、通行碼寫在程式碼或設定檔中，並避免使用預設通行碼，並要求使用者首次登入強制變更通行碼，並搭配帳號鎖定機制、通行碼複雜度及通行碼最短有效期限等防護策略。
- 建議通行碼採安全雜湊演算法處理，金鑰與機敏資料採取加密或其他適當措施，以及系統間通訊啟用TLS等傳輸加密機制。
- 資料庫、管理介面及診斷服務僅開放必要來源，正式環境關閉不必要服務，並確認除錯介面與詳細系統資訊不顯示於系統畫面。

四、記憶體使用不嚴謹(占比2.4%)

本類型漏洞共1個，為堆疊型緩衝區溢位漏洞，肇因於記憶體操作未妥善控管邊界，導致實際使用超出原配置範圍，進而影響到其他記憶體空間，可能造成程式異常、服務中斷，嚴重時甚至影響控制流程或造成執行任意程式碼。

防護建議：

- 系統複製、解析或處理通訊資料前，應先檢查資料長度與邊界，避免寫入超過緩衝區可容納之範圍。

焦點文章

- 優先採用具長度限制之安全函式或函式庫，汰換不安全字串與記憶體操作方式，並於必要時導入記憶體安全元件。
- 啟用位址空間配置隨機化(ASLR)、資料執行防止(DEP/NX)及堆疊金絲雀(Stack Canaries)等防護機制。

五、結語

本次統計數據顯示，我國市售系統與軟體產品廠商在「輸入驗證」與「身分鑑別與授權機制」等基礎安全面向，仍有明顯的改善空間，多屬於開發與設定階段即可預防之類型，顯示全面落實基礎資安實務之重要性。

建議優先修補可造成遠端程式碼執行、未授權存取及機敏資料外洩之漏洞，並強化輸入驗證、採行參數化查詢、完善伺服器端身分鑑別與逐項授權、落實憑證管理等相關安全設定。同時導入SAST與安全開發生命週期(SSDLC)，降低再次出現同類型漏洞之情況。

關鍵字：漏洞通報、TWCERT/CC、TVN

刊　　名　資安週報第 56 期
發 行 人　國家資通安全研究院　龔化中院長
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