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

資安週報

Cyber Security Weekly Newsletter

2026.08.13
057

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等七類量化指標

■ 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

元件高風險漏洞下降 帶動整體風險降低

本次針對曝險程度較高之100個A、B級公務機關進行EASM資安曝險檢測，前10大風險項目共計9,302項。其中，「元件高風險漏洞」以3,632項居首，「過時或弱加密協定」1,898項次之，「TLS憑證不受信任」1,580項位居第三。前三項合計7,110項，占前10大風險項目總數約76.4%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密協定及憑證管理等議題。相較上期9,436項，本期整體風險數量減少134項，降幅約1.4%，詳見圖1。

進一步分析主要風險變化情形，「元件高風險漏洞」仍為最大宗風險，數量由上期3,903項減至本期3,632項，降幅約6.9%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍為主要風險來源，該弱點可能造成原始碼洩漏或程式碼執行風險，建議升級至2.4.60以上之已修補版本。「過時或弱加密協定」由1,913項減至1,898項，降幅約0.8%；「TLS憑證不受信任」由1,520項增至1,580項，增幅約3.9%。另「未部署WAF」由729項減至725項，減幅約0.5%；「CSP設定不當」由940項增至980項，增幅約4.3%。

整體而言，本期外部曝險風險呈下降趨勢，主要受「元件高風險漏洞」數量減少所帶動；惟「TLS憑證不受信任」及「CSP設定不當」均呈上升，仍應持續強化憑證管理及網站安全標頭設定，以降低相關曝險風險持續增加之可能性。

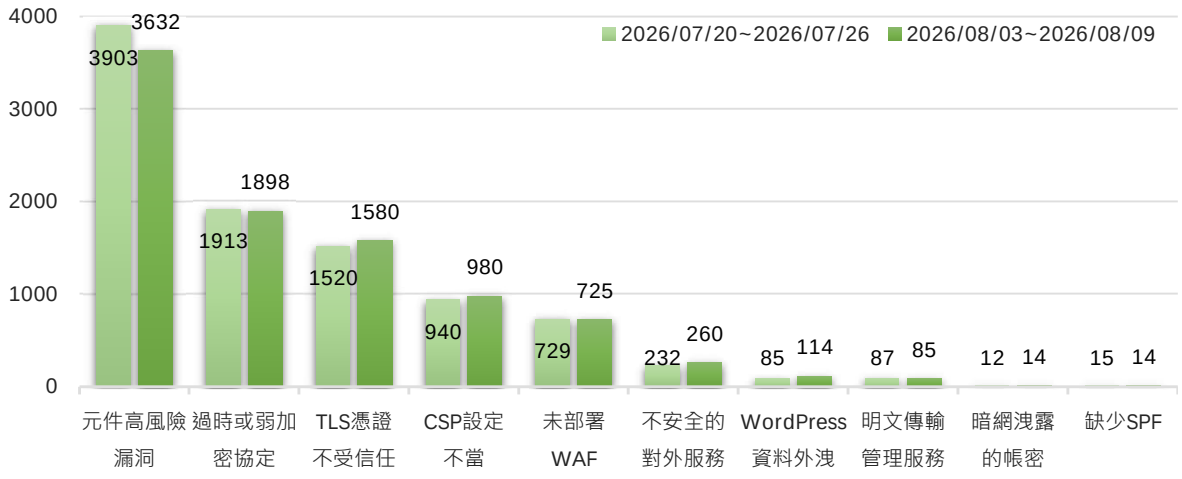


圖1 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施

- 盤點與修補對外服務之高風險元件漏洞，特別針對Apache HTTP Server等常見對外服務元件進行版本盤點與更新；如無法立即完成修補，應採取WAF、虛擬修補、限制存取來源或網路區隔等替代性防護措施
- 定期檢視TLS憑證有效性、憑證鏈及簽發來源，於憑證到期前完成更新，避免因憑證逾期、自簽憑證或憑證鏈不完整而造成不受信任情形
- 全面採用TLS 1.2以上版本之加密協定，停用TLS 1.0、TLS 1.1及安全性不足之加密套件與演算法，以降低通訊資料遭竊聽之風險
- 檢視並妥善設定Content-Security-Policy(CSP)等網站安全標頭，避免使用過度寬鬆之來源設定，並依實際業務需求限制可載入之腳本、樣式及其他外部資源，以降低XSS及惡意內容注入風險
- 持續檢視網站應用程式防火牆(WAF)部署情形，針對重要或高曝險之對外網站優先導入，並定期調整防護規則，以提升對常見Web攻擊之防禦能力

建議受測單位採取下列管理措施

- 建立對外資產及軟體元件清冊，定期盤點網站、主機、應用服務及使用版本，並掌握原廠安全公告與停止維護資訊，降低因版本過時而產生之曝險風險
- 建立弱點修補、複測及追蹤機制，依弱點嚴重程度訂定改善期限，並確認修補後風險項目確實消除，避免相同弱點長期或重複出現
- 建立TLS憑證生命週期管理機制，集中掌握憑證簽發、到期及更新狀態，並導入到期提醒或自動續期機制，以降低因憑證失效或管理疏漏所造成之風險
- 將CSP、TLS設定、WAF及其他網站安全組態納入系統上線與變更管理流程，於系統新增或設定異動後進行安全檢查，避免因組態變更產生新的外部曝險
- 持續強化系統維運及網站管理人員之資安教育訓練，提升其對元件漏洞管理、憑證生命週期、加密協定及網站安全標頭設定之安全意識與維運能力

■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

pgAdmin與Microsoft高風險漏洞應盡速修補

- pgAdmin 4存在高風險漏洞(CVE-2026-17566)[1]，類型為作業系統指令注入(OS Command Injection)，由於pgAdmin 4之資料匯入/匯出工具(Import/Export Data)未妥善處理SQL查詢，已通過身分鑑別之遠端攻擊者，可利用此漏洞執行任意程式碼。
- Microsoft Excel存在高風險漏洞(CVE-2026-62870)[2]，類型為使用釋放後記憶體(Use After Free)，未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼。

1. https://www.postgresql.org/about/news/pgadmin-4-v917-released-3356/
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62870

■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API存取控管失效 致個人資料外洩風險

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8/7止已累計265筆攻擊紀錄，本週新增弱點數量共20筆，分別為「無效的存取控管」8筆、「不安全的組態設定」4筆、「驗證機制失效」3筆、「注入攻擊」2筆、「軟體供應鏈失效」2筆及「加密機制失效」1筆，詳見圖2。

本週演練發現，高風險弱點為「無效的存取控管」。攻擊者透過瀏覽器開發者工具(Developer Tools)點選「Network」頁籤，檢視系統載入之「config.js」檔案內容，發現其中包含系統服務路徑，進一步瀏覽相關目錄與功能連結後，發現可直接存取查詢(Query)功能。攻擊者於該查詢介面調整查詢條件、回傳欄位及資料格式後執行查詢，發現系統未進行適當之身分驗證與存取權限檢查，即回傳相關資料，導致未經授權之使用者可取得相關個資。

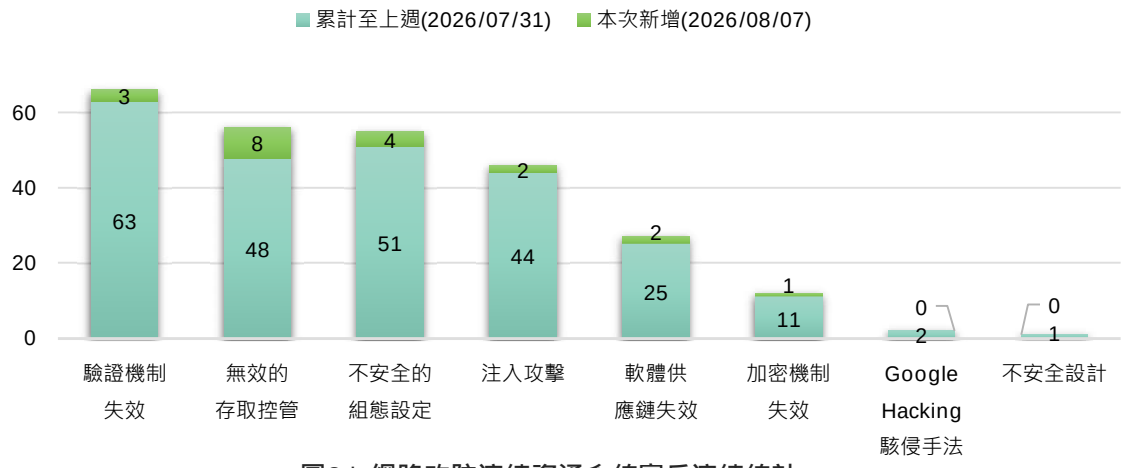


圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 針對後端API或功能應落實身分鑑別與授權機制，避免未經授權使用者直接存取或透過竄改查詢參數取得資料
- 應依最小權限原則限制API可查詢之資料範圍與欄位，針對個人資料等敏感資訊進行適當遮罩或去識別化處理，降低敏感資料外洩風險
- 定期檢視與檢測系統功能與API之權限控制，降低系統因版更或調整可能造成權限控制失效弱點

■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14.6%，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13.4%，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網路資產資訊蒐集活動。觀察到的主要手法包括主動式掃描、IP區段掃描，以及IP 位址資訊蒐集。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，以識別可存取主機、開放埠及服務資訊，並進一步蒐集與目標相關的 IP 位址及網路基礎設施資訊，藉此掌握對外暴露資產與潛在攻擊入口。此類活動通常具高度自動化及廣泛探測特性，可協助攻擊者建立目標資產輪廓，並作為後續漏洞掃描與初始入侵的重要依據。

建議機關持續監控異常掃描流量及可疑來源，定期盤點對外暴露的 IP 與網路服務，並結合威脅情資進行來源分析與阻擋，以提前辨識攻擊者的偵查活動並降低後續入侵風險。

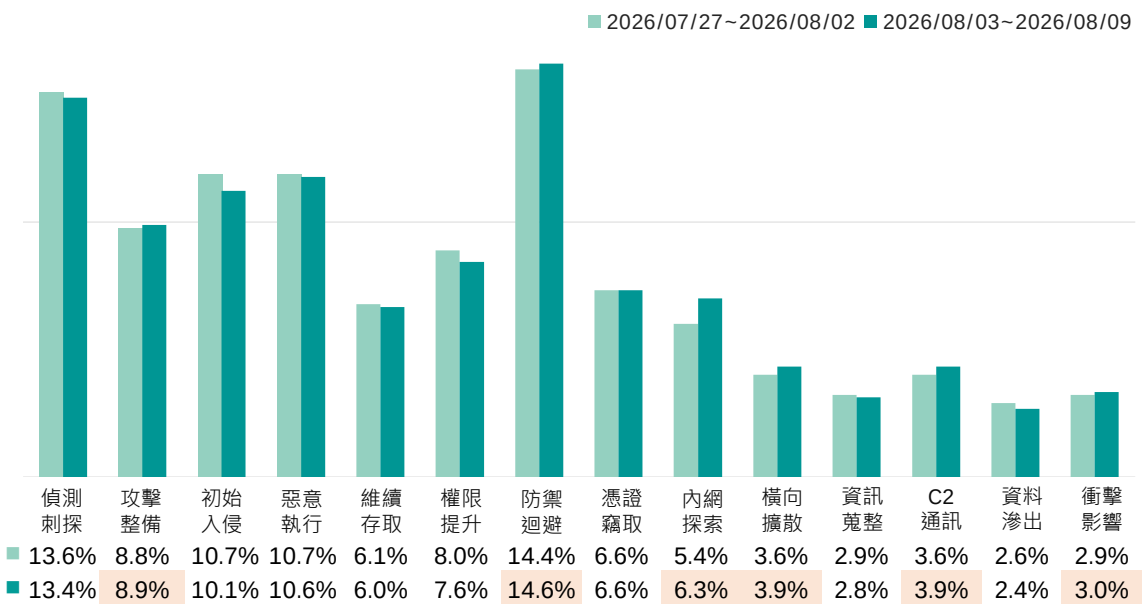


圖3 | 資安聯防監控攻擊階段統計

防護建議

建議機關採取下列防護措施

防禦迴避(Defense Evasion)

	導入並強化端點偵測與防護機制(EDR)
	加強系統指令與操作紀錄稽核，避免紀錄遭任意刪除或停用
	限制高風險系統工具及指令的使用權限，降低合法工具遭濫用風險
	落實特權帳號與最小權限管理，強化異常操作監控

偵測刺探(Reconnaissance)

	持續監控異常掃描流量、IP 區段掃描及可疑來源
	定期盤點對外暴露的 IP、通訊埠及網路服務，降低非必要曝險
	結合威脅情資分析可疑來源 IP，適時進行封鎖或存取限制
	建立掃描與探測行為告警機制，及早發現攻擊者前期偵查活動

■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

AI應用平台與套件成攻擊熱點

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73.72%、「遠端控制」服務攻擊占比22.91%，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75.59%。「遠端控制」服務亦有19.53% 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服務系統比例下降主因為GeoServer程式碼注入漏洞之CVE-2024-36401，遭攻擊次數下降導致。

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。

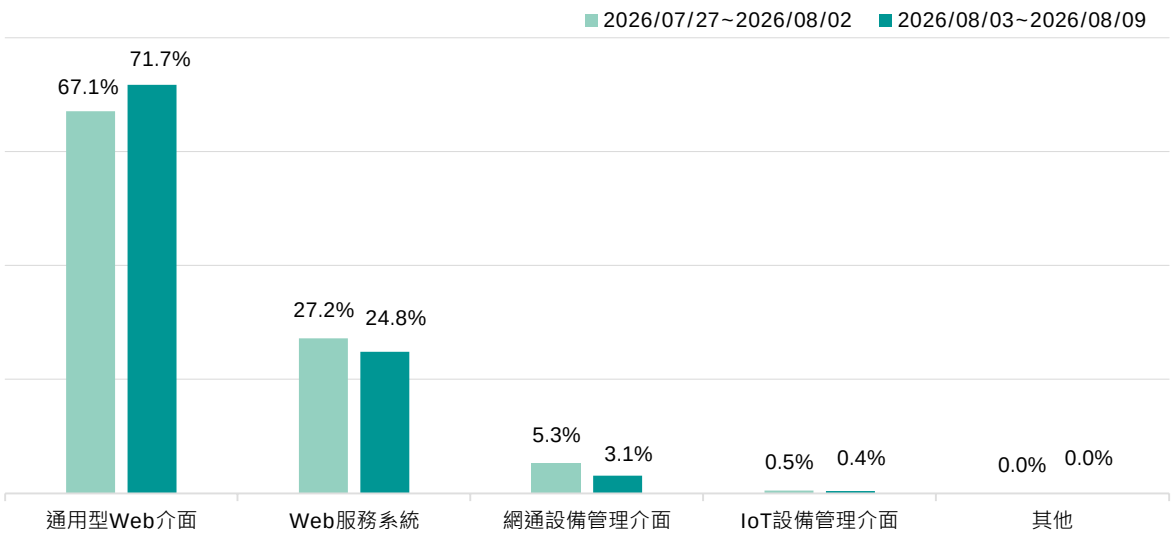


圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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1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輸入驗證不當漏洞、指令注入漏洞、身分驗證繞過漏洞及越界讀取漏洞，攻擊目標涵蓋視覺化工作流程自動化工具、大模型API統一介面與代理伺服器工具、網站主機伺服器管理系統、程式遞送控制器(ADC&Gateway)及企業級終端裝置管理與資安防護系統。

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1年漏洞排行列表

排名			漏洞編號	受影響產品	CVSS 3.x Base Score	已知遭利用漏洞 (KEV)
■	1	↑3	CVE-2026-21858[1]	n8n	10	X
■	2	↑new	CVE-2026-42271[2]	LiteLLM	8.8	✓
■	3	↑new	CVE-2026-41940[3]	cPanel & WHM	9.8	✓
■	4	↑new	CVE-2026-3055[4]	NetScaler ADC & Gateway	9.8	✓
■	5	↑new	CVE-2026-1603[5]	Ivanti Endpoint Manager	8.6	✓

類型 ■ 輸入驗證不當漏洞 ■ 指令注入漏洞 ■ 身分驗證繞過漏洞 ■ 越界讀取漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2026-21858
2. https://nvd.nist.gov/vuln/detail/CVE-2026-42271
3. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
4. https://nvd.nist.gov/vuln/detail/CVE-2026-3055
5. https://nvd.nist.gov/vuln/detail/CVE-2026-1603

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

API與Token安全應從「誰能取得、能存取什麼、能使用多久」三面向控管

本週總計接獲22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系統遭入侵、未經授權存取及異常連線占多數，詳見圖6。本週發現機關網站API存在身分驗證及存取控制缺失，攻擊者可在未經適當授權情況下取得有效存取憑證，並利用該憑證呼叫API取得大量網站資料；另亦發現攻擊者透過腳本使用網站核發之Token持續查詢及下載資料。

參考OWASP API Security建議，API安全除確認Token有效外，仍應進一步限制使用者可存取之功能、資料範圍及使用方式，並妥善管理Token生命週期。建議優先檢視下列事項：

- 憑證核發機制：確認Token僅於完成必要身分驗證後核發，不得由未授權頁面、API回應或前端程式直接取得有效憑證。
- API存取權限：每次API請求均應依帳號、角色及業務權限限制可使用功能與資料範圍，並測試修改資料、頁碼或查詢條件後，是否可能取得非授權資料。
- 檢視Token生命週期：確認Token具合理有效期限及失效機制，並於登出、密碼變更或帳號停用後，原Token是否仍可使用；另應避免Token暴露於網址、網頁原始碼或不必要之系統紀錄。
- 檢視大量存取機制：應針對大量查詢、連續翻頁及批次下載設定限制或異常告警。

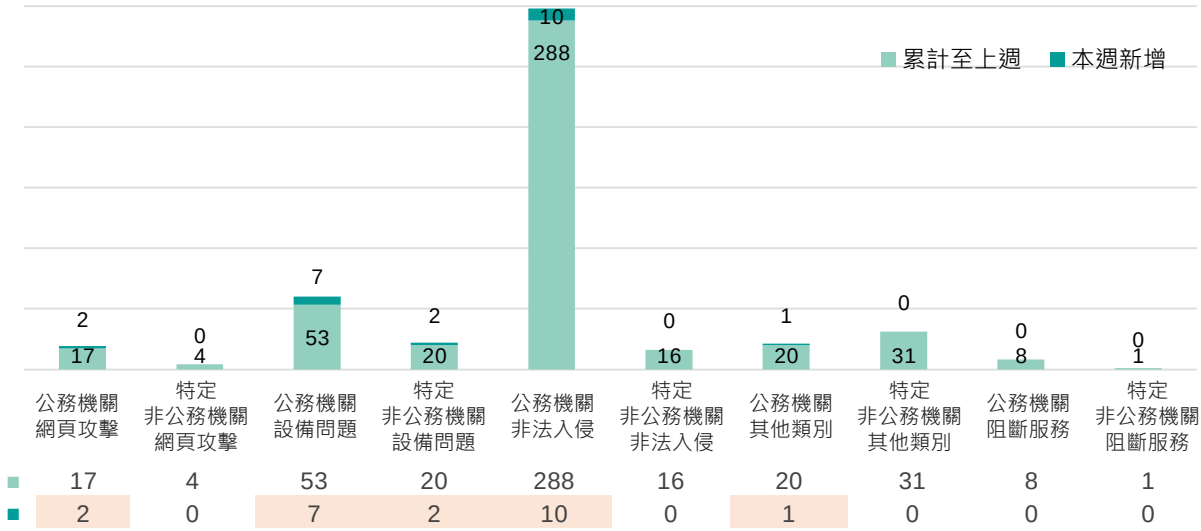


圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

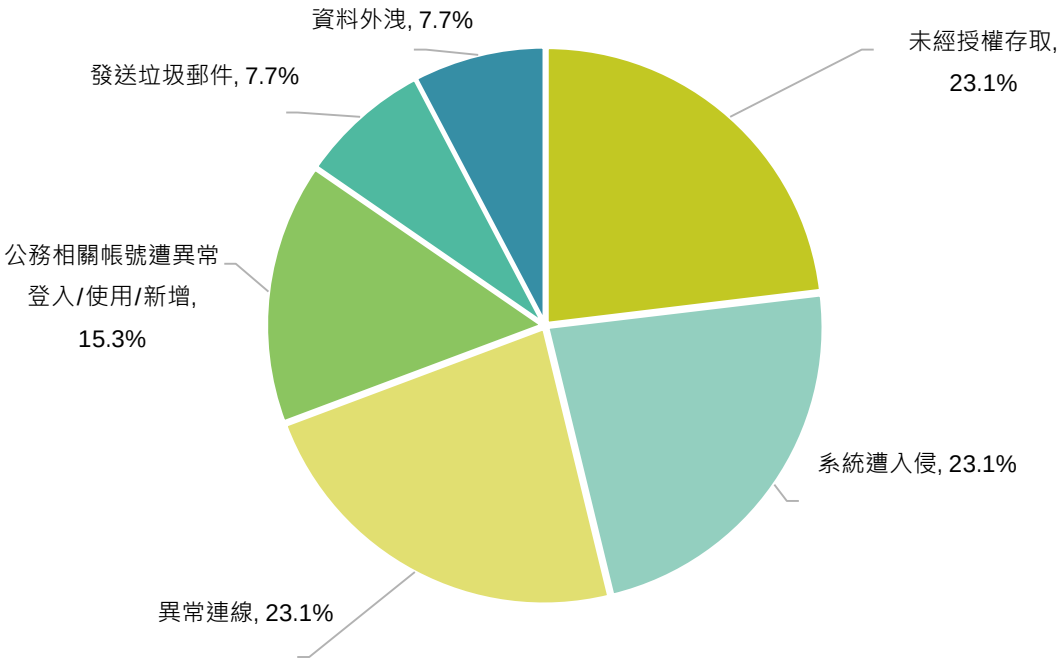


圖6 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者濫用有效Token批次存取敏感資料 ➢ API權限控管不足導致大量資料遭未授權下載	➢ 強化Token核發驗證機制，僅於完成必要身分驗證後提供有效憑證 ➢ 落實API細緻權限控管，依帳號角色限制可存取功能與資料範圍 ➢ 建立Token生命週期管理，落實有效期限、撤銷及帳號異動後失效 ➢ 針對大量查詢與批次下載設定速率限制、異常告警及行為監控

5間民間企業揭露重大資安訊息

本週5家民間企業發布重大訊息，產業類別為通信網路業、生技醫療業、電腦及週邊設備業、光電業，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
聯合光纖通信股份有限公司	2026年08月03日	聯光通公司於2026年8月3日收到資訊系統遭勒索病毒攻擊訊息，已立即檢視內部相關資安紀錄並加強相關防護機制，目前所有資訊系統陸續恢復正常運作。後續將持續密集監控，且強化網路與資訊系統基礎架構之管控，以確保資訊系統安全。
藥華醫藥股份有限公司	2026年08月03日	藥華藥及泛泰醫療子公司之部份資訊系統遭受駭客網路攻擊，初步評估對公司營運無重大影響。目前已委請外部資訊安全技術公司及專家共同處理，後續依程序向主管機關通報、持續提升網路與資訊基礎架構之安全管控，以確保資訊安全。
尼得科超眾科技股份有限公司	2026年08月04日	尼得科超眾於2026年6月22日偵測到部分伺服器遭受網路勒索病毒攻擊，致使包含ERP在內之部分資訊系統無法正常運作。宣稱實施攻擊集團於暗網公開部分資料夾及檔名清單截圖，經委託外部專業機構進行數位鑑識調查，未能證明該等資料流向外部之明確技術證據。雖未能完全排除資訊外洩之可能性，後續將持續密切關注狀況並維持監控。

公司名稱	發布時間	事件說明
州巧科技股份有限公司	2026年08月05日	州巧公司及重要子公司(蘇州州巧、廈門州巧及越南州巧)偵測部分資訊系統遭駭客攻擊時，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。目前正對相關系統進行全面性的資安掃描與檢測，確保資訊安全無虞後，將利用日常備份資料陸續復原系統運作，經初步評估對公司營運無重大影響。完成相關安全漏洞修復後，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，確保資訊系統穩定運作及資訊安全。
逸達生物科技股份有限公司	2026年08月07日	逸達公司資訊系統遭受駭客網路攻擊，已啟動資訊安全防禦機制，並委請外部資訊安全技術公司及專家共同處理，後續依程序向主管機關通報，初步評估對公司營運暫無重大影響，將持續提升網路與資訊架構之安全管控，以確保資訊安全。

■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

產品服務風險回升 專業背書與限時優惠話術擴散

本週金融投資占比由前週12.4%降至9.2%，減少3.2個百分點，詳見圖7。相關話術由低額開戶、免費模擬交易及投資社群導流，轉向財商課程、免費線上營及理財諮詢，並運用「華爾街操盤手」、「財務規劃顧問」、「限時優惠」及「一對一諮詢」等說法吸引民眾。整體顯示，直接投資招攬有所降溫，投資教學與免費課程仍持續扮演接觸及導流角色。

身分冒充占比維持平穩，由前週9.9%微降至9.8%。相關內容持續運用專科醫師、國外研發團隊、實驗證明及知名講師等專業身分建立信任，透過「醫師推薦」、「日本團隊親研」、「實驗證實」及「專業顧問」等說法營造權威背書。此類專業身分包裝持續降低民眾戒心，使身分冒充內容維持一定能見度。

產品服務占比由前週77.7%升至81.0%，增加3.3個百分點，再度突破八成。高風險商品涵蓋灰甲修護、牙齒修護、痛風凝膠、體重管理產品、兒童玩具、清潔用品及服飾鞋款等。常見手法包括境外品牌與技術背書、醫師推薦、精確療效數字、安全無副作用及限時折扣，再透過留言、私訊或陌生網址引導購買。保健商品與生活消費品並行擴散，推升產品服務成為本週最主要的高風險類型。

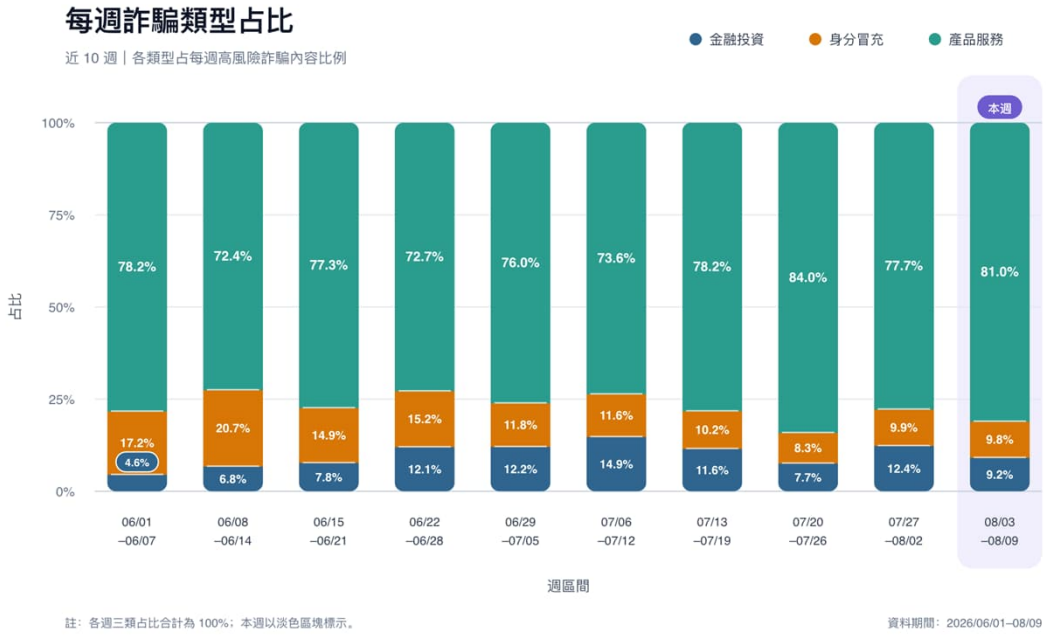


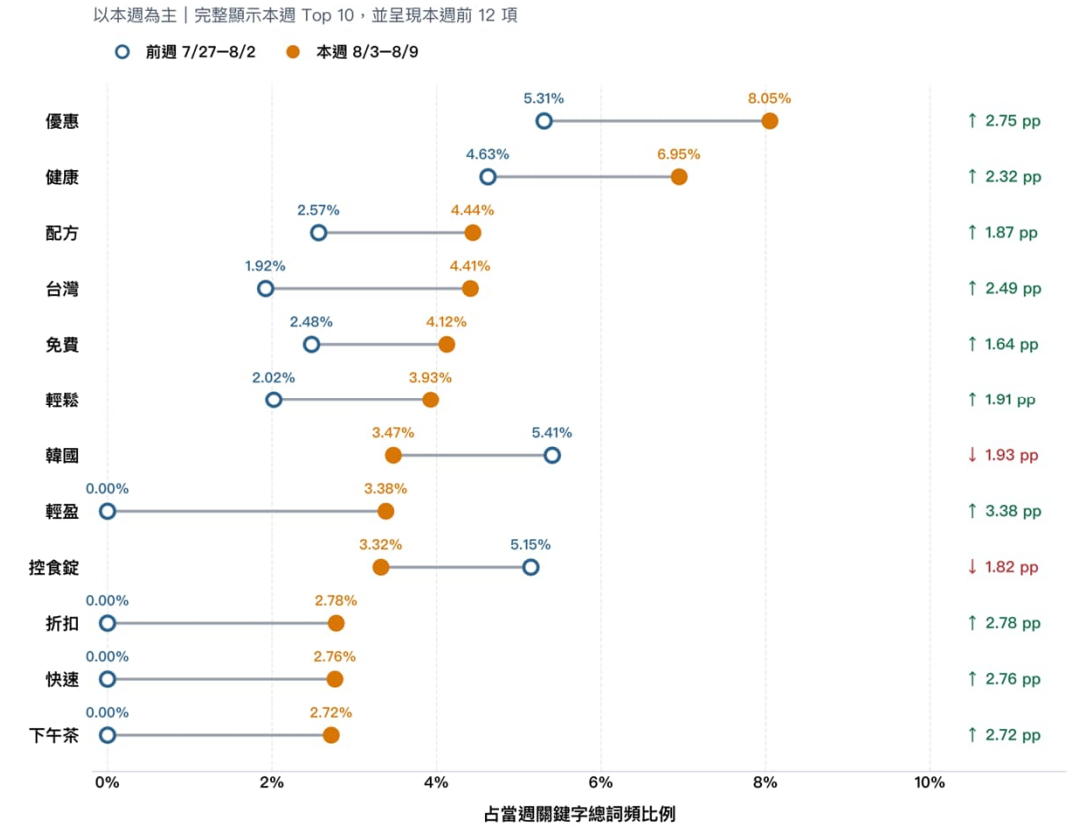
圖7 | 每週詐騙類型占比

「優惠」占比由前週5.31%升至8.05%，增加2.74個百分點，升至本週首位。相關話術由中古車貸款轉向財商課程，結合倒數期限、限時優惠及專業講師形象，營造促銷急迫感。

保健醫療話術明顯升溫。「健康」由4.63%升至6.95%，主要運用醫師推薦及境外品牌包裝修護產品；「配方」由2.57%升至4.44%，著重牙齒修護、實驗證明及安全無副作用等訴求。此類內容透過專業身分、外國技術與具體功效描述強化可信度。

「台灣」由1.92%升至4.41%，增加2.49個百分點，常以「台灣車友圈瘋傳」、「本島免運」及「現貨秒發」等在地化說法建立熟悉感。「免費」由2.48%升至4.12%，由免費投資模擬轉向免費AI線上營及一對一諮詢；「輕鬆」亦由2.02%升至3.93%，反映零成本、低門檻及容易操作等訴求持續降低民眾戒心。

詐騙關鍵字占比週比變化



註：占比＝關鍵字出現次數 ÷ 當週檔案所列關鍵字出現次數總和；pp 為百分點。

圖8 | 詐騙關鍵字占比週比變化

體重管理仍是本週重要話術。「韓國」由5.41%降至3.47%，「控食錠」由5.15%降至3.32%，「輕盈」則以3.38%新進前十名，相關內容結合境外熱銷、女團形象、植物纖維及安全認證包裝產品。「折扣」亦以2.78%進入前十名，顯示促銷優惠、健康功效、便利體驗及境外形象共同構成本週主要高風險話術。

焦點文章

CRA漏洞通報義務倒數：ENISA單一通報平台最新進展

歐盟《網路韌性法》（Cyber Resilience Act, CRA）漏洞通報義務將於2026年9月11日正式生效；歐盟網路安全局（European Union Agency for Cybersecurity, ENISA）亦正建置「單一通報平台」（Single Reporting Platform, SRP），作為企業與其他組織通報漏洞與資安事件的重要窗口。隨著通報義務生效日接近，組織關注焦點從法遵合規準備，漸轉向漏洞通報程序與實際執行層面。本文即因應此關切，整理CRA漏洞通報義務，並彙整至8月3日ENISA公布之SRP最新資訊。

一、不是所有漏洞都要通報，CRA通報範圍鎖定2種類型

SRP是由ENISA建置的單一線上通報平台，目的是協助企業履行CRA規定的漏洞與資安事件通報義務。CRA第14條的強制通報範圍主要鎖定以下2種類型[1]。

第一類是「活躍已被利用的漏洞」（actively exploited vulnerability），指已有可靠證據顯示惡意行為者曾在未經系統權限者授權的情況下實際利用該漏洞[2]。

第二類是「對產品安全造成影響的嚴重事件」（severe incident），如該事件嚴重影響某產品保護敏感或重要資料或功能之可用性、真實性、完整性或機密性的能力；或者導致惡意程式碼被植入或執行於產品本身，及產品使用者的網路與資訊系統的情形[3]。

二、誰負責向SRP通報？製造商是主要義務者

CRA的漏洞通報義務，原則由製造商負責[4]。但實際責任並不限於傳統認知中的原廠，依CRA第21條，進口商或經銷商若改以自身名稱或品牌將產品投放歐盟市場，或對產品進行「實質修改」，即承擔與製造商相同的漏洞通報義務[5]。另外，開源軟體管理者（open-source software stewards）也是通報義務的角色之一，如果漏洞涉及開源軟體管理者參與開發的產品，或嚴重事件影響其所開發的資訊系統，也需進行通報並通知受影響的使用者[6]。

焦點文章

三、何時向SRP通報？採24小時、72小時及最終報告3階段

首先，24小時通報的重點並不要求企業提供完整調查報告，而是先掌握事件輪廓。企業登入SRP後，可建立新的漏洞或事件案件，並選擇「活躍已被利用的漏洞」或「嚴重事件」。目前SRP系統允許企業儲存草稿，但只有正式提交後，才算完成通報。在此階段，企業應至少掌握受影響產品資料；產品名稱及版本；企業知悉事件的時間；漏洞或事件的初步性質；產品提供的成員國；已知的CVE或EUVD編號；是否涉及惡意或非法行為；資訊敏感程度等資料。[7]

在72小時的階段，須補足產品、影響與緩解措施的資訊。若屬漏洞，企業須說明漏洞性質、利用方式、受影響產品與版本、已採取的修補或緩解措施，以及使用者可採取的因應方法。若屬嚴重事件，則須補充事件發生及偵測時間、初步影響評估、受影響的產品、資料或功能，以及已完成或進行中的處置措施。

在最終報告階段，則依漏洞與事件採不同期限。對活躍已被利用的漏洞，最終報告原則上應在修正或緩解措施可供使用後14日內提交，內容應包含完整漏洞說明、嚴重程度、產品及使用者影響、修補方式與取得方法。對嚴重事件，最終報告原則上應在72小時通知後一個月內完成，須說明事件經過、根因或威脅類型、影響範圍、復原措施及防範作法。

四、如何向SRP通報？

當企業確定產品發生CRA規定的活躍已被利用的漏洞，或出現影響產品資安的嚴重事件後，應透過ENISA建置的「單一通報平台」（SRP）提交通知[8]。製造商原則上只需提交一次資料，再由負責協調的CSIRT將通報資訊分送至相關成員國的CSIRT及市場監督機關[9]。

實際通報時，企業須先以EU Login帳戶登入，並依CRA第14條第7項確認負責受理及協調的CSIRT[10]。若製造商在歐盟設有主要營業據點，原則上由所在地CSIRT負責；若未在歐盟設立主要據點，則依授權代表、進口商、經銷商或使用者數量最多之成員國為順序判定[11]。目前依ENISA說明，企業已可建立EU Login帳戶，但ENISA補充因各國CSIRT採取的驗證程序可能不同，為避免大量預先註冊增加驗證負擔，ENISA建議可在需要提交通報時再進行註冊[12]。

焦點文章

另針對希望將通報作業直接整合內部漏洞管理系統，或擁有大量產品需要通報的企業而言，在系統自動化通報與對接的問題上，依ENISA目前說明，SRP尚未提供應用程式介面（API），因此在初期仍可能須半自動或手動輸入資訊[13]。

五、SRP不是最後一哩路：真正挑戰仍在企業內部流程

SRP解決的是跨國傳遞漏洞資訊的問題，而能否在時限內進行通報，仍有賴企業建立一套完善有效的內部運作流程。為提前因應準備，首先宜提前掌握自身各項產品中硬體、軟體、韌體元件間的依賴關係，建立產品名稱、型號、版本、支援狀態、銷售地及進口與經銷商資訊的產品清冊，以利掌握產品狀態。

此外，亦可預先依ENISA所提供的各階段所需通報欄位，提前建立包括產品資訊、可能受影響版本、漏洞資訊描述、已知利用活動、影響範圍、涉及成員國、預期修補措施等欄位框架，以利在初期資訊不完整時，能夠快速取得早期預警內容。

最後，因目前SRP尚未提供API，企業內部雖可自動化完成資訊蒐集，但正式通報時仍可能須由人員實際進行操作，因此建議可依照各階段通報要求，進行桌上模擬演練，測試能否在時間內完成漏洞分類、通報決策及初步填報等，實際驗證能否在資料有限、時區不同、長假期間及關鍵人員請假或不在場時，仍能依程序完成通報。

參考資料：

[1] European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/2847 (Cyber Resilience Act), Article 14. Official Journal of the European Union. Retrieved August 3, 2026, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402847.
[2] Regulation (EU) 2024/2847, Article 3, point (42).
[3] Regulation (EU) 2024/2847, Article 3, points (43) and (44).
[4] Regulation (EU) 2024/2847, Article 14.
[5] Regulation (EU) 2024/2847, Article 21.
[6] Regulation (EU) 2024/2847, Article 24.
[7] European Union Agency for Cybersecurity. (2026, August 3). Frequently asked questions: 16. What are the data fields to be filled in the reporting template? Retrieved August 3, 2026, from https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions.

焦點文章

[8] Regulation (EU) 2024/2847, Article 16(1).
[9] Regulation (EU) 2024/2847, Article 16(2).
[10] European Union Agency for Cybersecurity. (2026, July 31). CRA Single Reporting Platform factsheet. Retrieved August 3, 2026, from https://www.enisa.europa.eu/media/57221.
[11] Regulation (EU) 2024/2847, Article 14(7).
[12] European Union Agency for Cybersecurity. (2026, August 3). Frequently asked questions: 9. How will the platform be accessible and how will the registration process work? Retrieved August 3, 2026, from https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions.
[13] European Union Agency for Cybersecurity. (2026, August 3). Frequently asked questions: 15. Can the notification workflow be automated for large number of notifications from one manufacturer? Retrieved August 3, 2026, from https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions.

關鍵字：歐盟網路韌性法、漏洞通報、單一通報平台

刊　　名　資安週報第 57 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