



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

整體曝險持續下降 元件高風險漏洞仍居首位

重大漏洞

SonicWall、綠色運算、MongoDB、Splunk、Veeam及Zimbra
高風險漏洞應盡速修補

實兵演練

實兵演練揭露系統功能資訊揭露 致個人資料遭未授權存取風險

聯防監控

偵測刺探高居首位 防禦迴避仍具威脅

蜜罐誘捕

網站主機伺服器管理系統及程式遞送控制器(ADC&Gateway)成攻擊熱點

事件通報

網站部署應避免將敏感設定檔暴露於公開路徑

網路巡查高風險詐騙

金融投資與身分冒充回升 產品服務仍占首位

焦點文章

從賽事經驗建構台灣資安人才生態圈的實踐

2026.09.10

061

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

整體曝險風險持續下降 元件高風險漏洞仍居首位

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8,415項。其中，「元件高風險漏洞」以3,316項居首，「過時或弱加密協定」1,606項次之，「TLS憑證不受信任」1,315項位居第三。前三項合計6,237項，占前10大風險項目總數約74.1%，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9,040項，本期整體風險數量減少625項，降幅約6.9%，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3,428項減至本期3,316項，降幅約3.3%。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。此外，本期觀察到Apache Tomcat所使用之Apache JServ Protocol相關弱點(CVE-2020-1938)、Windows網域的Netlogon驗證相關弱點(CVE-2020-1472)與Drupal核心相關弱點(CVE-2020-13671)數量較上期減少，顯示部分機關已逐步完成相關弱點改善。「過時或弱加密協定」由1,811項大幅減至1,606項，降幅約11.3%；「TLS憑證不受信任」由1,536項大幅減至1,315項，降幅約14.4%。另「未部署WAF」由799項減至766項，降幅約4.1%；「CSP設定不當」由1019項降至985項，降幅約3.3%。

整體而言，本期外部曝險風險呈下降趨勢，各類風險數量均較上期減少。其中，「TLS憑證不受信任」及「過時或弱加密協定」降幅最為明顯，顯示相關改善措施已具初步成效；惟「元件高風險漏洞」仍為最大宗風險，且「未部署WAF」及「CSP設定不當」仍有一定數量，建議持續推動高風險元件更新、WAF部署及CSP設定優化，以進一步降低外部曝險風險。

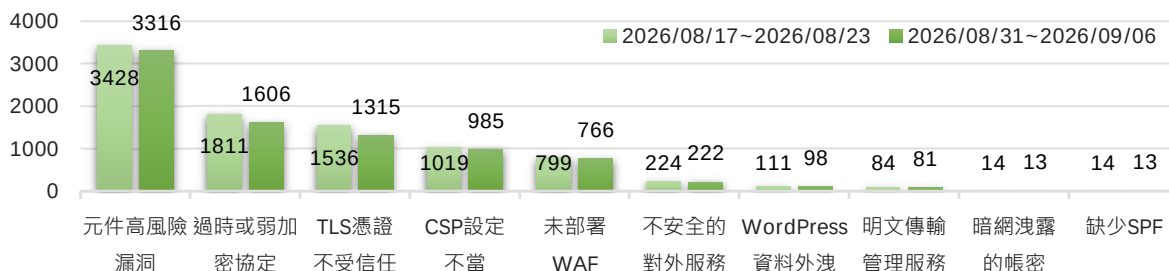


圖1 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施

- 優先修補對外服務所使用元件之高風險漏洞，並依原廠安全公告更新至已修補版本；如短期內無法完成升級，應採取WAF、虛擬修補、來源存取限制或網路區隔等補償性措施，以降低漏洞遭利用之風險
- 依據IETF RFC 10015，檢視TLS 1.2所使用之金鑰交換機制，停用較舊或安全性較低之方式，並優先採用ECDHE等具前向保密性之安全機制，以強化加密通訊安全
- 強化TLS憑證管理，定期檢視憑證有效期限、信任鏈及憑證狀態，並建立到期通知及自動續期機制，避免因憑證失效造成服務異常或安全風險
- 定期檢視網站CSP及WAF等防護設定，並依系統功能及實際業務需求調整安全政策，以降低跨網站腳本、惡意請求及其他

Web攻擊風險

建議受測單位採取下列管理措施

- 建立並定期維護對外資產清冊，納管IP、網域、系統元件及憑證等資訊，以掌握各項資產之用途、版本及使用情形
- 建立高風險漏洞之修補、追蹤及複測機制，依漏洞嚴重程度訂定修補期限，並於完成修補後進行複測，確認改善措施有效落實
- 定期盤點系統所使用之軟體及第三方元件版本，持續追蹤原廠安全公告及CVE弱點資訊，並適時進行版本更新，降低使用已停止支援或存在已知弱點元件之風險
- 將漏洞修補、憑證更新、安全設定調整及後續複測等要求納入委外維運管理，明確訂定處理時限、責任分工及追蹤方式，以確保各項改善措施確實執行

■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

SonicWall、綠色運算、MongoDB、Splunk、Veeam及Zimbra高風險漏洞應盡速修補

- SonicWall NetExtender Linux 存在路徑遍歷(Path Traversal)漏洞(CVE-2026-66152)[1]，未經身分鑑別之遠端攻擊者，可利用檔案解壓縮元件，以root權限寫入任意檔案。
- 綠色運算NUMail存在作業系統指令注入(OS Command Injection)漏洞(CVE-2026-82082)[2]，未經身分鑑別之遠端攻擊者可注入任意作業系統指令並於伺服器上執行。
- MongoDB BI Connector ODBC Driver存在整數溢位(Integer Overflow)漏洞(CVE-2026-19001)[3]，未經身分鑑別之遠端攻擊者可藉由傳入過長之名稱參數，造成緩衝區溢位，進而造成記憶體毀損與程式異常終止，並可能執行任意程式碼。
- Splunk Enterprise存在多項高風險安全漏洞(CVE-2026-76253、CVE-2026-76310至CVE-2026-76317、CVE-2026-76319、CVE-2026-76335及CVE-2026-76350至CVE-2026-76352)[4]，其中最嚴重之CVE-2026-76310為不當存取控制(Improper Access Control)漏洞，未經身分鑑別之遠端攻擊者若持有嵌入式報表令牌(Token)，可下載相關搜尋工作的派送封存檔，並從中取得工作階段相關資訊，進而存取報表擁有者可存取之資料，並影響系統完整性。若報表擁有者具admin角色時，攻擊者甚至可執行管理作業。
- Veeam ONE存在2項高風險安全漏洞(CVE-2026-64633與CVE-2026-65641)[5][6]，類型分別為程式碼注入(Code Injection)與身分鑑別繞過(Authentication Bypass)。前者可使未經身分鑑別之遠端攻擊者於代理主機(Agent Host)執行程式碼，後者可使未經身分鑑別之遠端攻擊者迫使服務帳戶對外發起SMB身分鑑別。
- Zimbra Collaboration存在作業系統指令注入(OS Command Injection)漏洞(CVE-2026-73570)[7]，當系統安裝選用套件zimbra-snmp並啟用SNMP通知功能時，未經身分鑑別之遠端攻擊者可藉由傳送特製SMTP請求，以Zimbra使用者權限執行任意作業系統指令，該漏洞已遭駭客利用。

1. <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0013>
2. <https://www.twcert.org.tw/tw/cp-132-11144-45c6a-1.html>
3. <https://github.com/mongodb/mongo-bi-connector-odbc-driver/releases/tag/v1.4.9>
4. <https://advisory.splunk.com/advisories/SVD-2026-0801>
5. <https://www.veeam.com/kb4892>
6. <https://www.veeam.com/kb4905>
7. https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

■ 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

實兵演練揭露系統功能資訊揭露 致個人資料遭未授權存取風險

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9/4止已累計329筆攻擊紀錄，本週新增弱點數量共23筆，分別為「不安全的組態設定」5筆、「加密機制失效」5筆、「軟體供應鏈失效」5筆、「注入攻擊」3筆、「驗證機制失效」3筆及「無效的存取控管」2筆，詳見圖2。

本週演練發現，部分系統存在「無效的存取控管」弱點。攻擊者透過Dirsearch工具掃描網頁目錄，發現系統Readme檔案，瀏覽檔案內容後取得系統功能路徑格式，進一步依該格式組成請求進行測試，發現系統未落實適當之身分驗證與存取權限控管，即回傳相關資料，攻擊者因此取得包含姓名、身分證字號、地址及電話等個人資料，造成敏感個資遭未授權存取之風險。

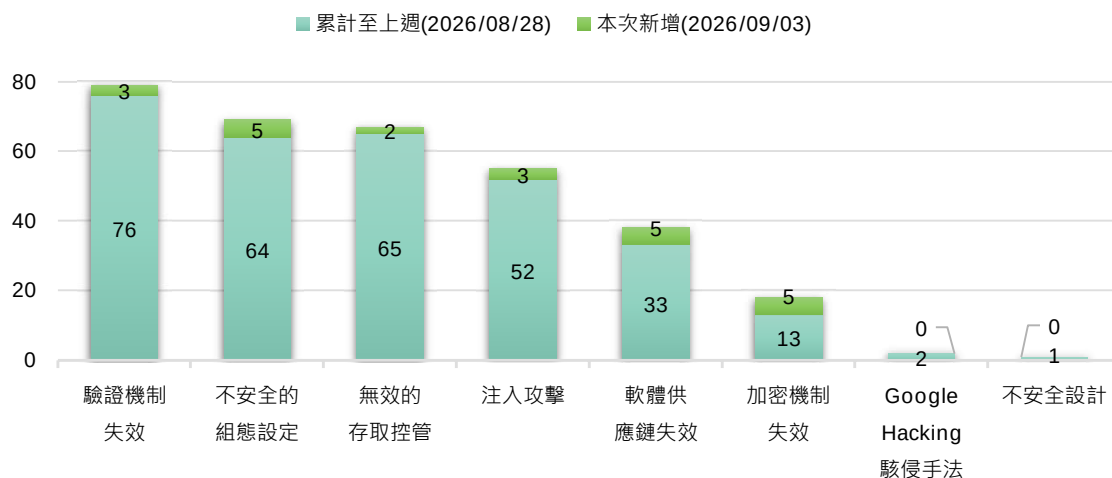


圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應針對系統各項功能或API落實身分鑑別與授權機制，避免未經授權使用者透過直接存取功能路徑或竄改請求參數取得系統資料
- 針對姓名、身分證字號、地址及電話等個人資料，應依資料敏感程度採取適當之遮罩、去識別化或其他保護措施，降低敏感個資遭未授權取得之風險
- 應檢視系統文件與公開資料，避免揭露系統功能路徑、API格式及參數等資訊，降低遭推測與未授權存取之風險

■ 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

偵測刺探高居首位 防禦迴避仍具威脅

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。「偵測刺探」為最常見攻擊手法，占比13.2%，顯示攻擊者持續加強對目標環境的前期偵查與弱點探測活動，以掌握潛在攻擊入口並提高後續入侵成功率。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外部網段及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，並進一步針對對外系統進行漏洞掃描，尋找可供利用的已知弱點。此類活動通常呈現由廣泛網路掃描逐步聚焦至特定系統與弱點的特徵，為後續漏洞利用及初始入侵的重要前置作業。建議機關持續監控異常掃描流量及可疑來源，定期盤點對外暴露資產並落實高風險漏洞修補，同時結合威脅情資進行掃描來源分析與阻擋，以提前辨識攻擊者的偵查活動並降低後續入侵風險。

「防禦迴避」事件本週占比為12.7%，為本週占比次高的攻擊階段，顯示攻擊者持續透過規避監控、隱藏操作軌跡及降低行為可視性等方式，以避免惡意活動遭安全機制偵測。觀察到的主要手法包括削弱指令歷程記錄、間接指令執行、以及清除指令歷程。攻擊者可能透過停用或修改指令歷程記錄功能，降低系統對操作行為的可追溯性，並利用合法程序或系統元件間接執行指令，以規避既有安全偵測機制；部分活動亦會於完成操作後清除Shell 或指令歷程，藉此隱藏攻擊軌跡並增加事件調查難度。此類行為具高度隱蔽性，可能影響後續事件追蹤與鑑識分析。

建議機關強化指令執行及日誌異常變更行為的監控，落實集中式日誌保存與完整性保護，並針對異常程序鏈及間接指令執行建立偵測機制，以降低攻擊者規避防禦及隱匿活動的風險。

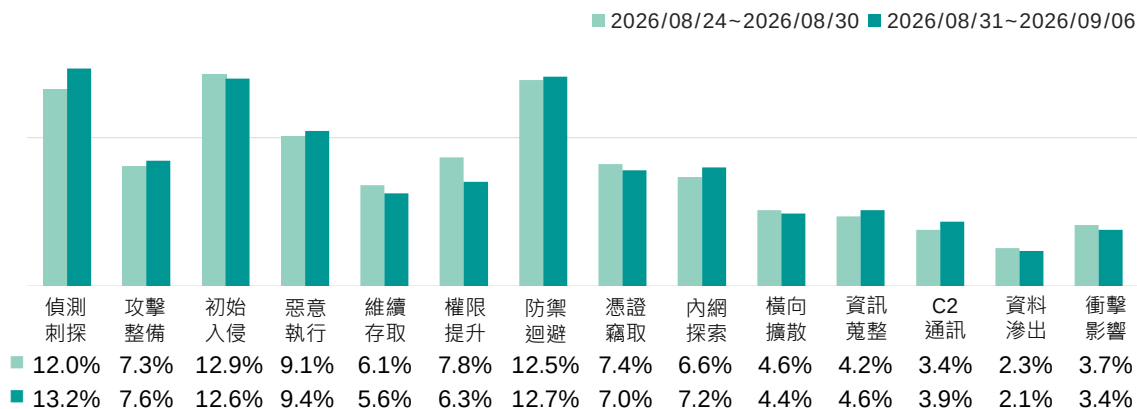


圖3 | 資安聯防監控攻擊階段統計



防護建議

建議機關採取下列防護措施



偵測刺探 (Reconnaissance)



持續監控異常掃描流量、IP 區段掃描及漏洞掃描行為



定期盤點對外暴露資產、服務及開放埠，降低不必要的攻擊面



優先修補對外系統之高風險及已知遭利用漏洞



結合威脅情資識別惡意掃描來源，適時進行封鎖或存取限制



建立掃描行為告警機制，及早發現由廣泛掃描轉向特定系統的可疑活動



防禦迴避 (Defense Evasion)



強化 Shell、PowerShell 及系統指令執行行為之監控與稽核



監控指令歷程遭停用、修改或清除等異常行為



採集中式日誌保存，並建立日誌完整性保護及適當留存機制



針對異常父子程序、程序鏈及間接指令執行建立偵測規則



限制非必要管理工具及高權限操作，降低攻擊者利用合法工具規避偵測的機會

■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

網站主機伺服器管理系統及程式遞送控制器(ADC & Gateway)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74.12%、「遠端控制」服務攻擊占比21.72%，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80.34%。「遠端控制」服務亦有16.63%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服務系統比例大幅下降主因為開放管理基礎架構 (OMI) 遠端執行程式碼漏洞之 CVE-2021-38647，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。

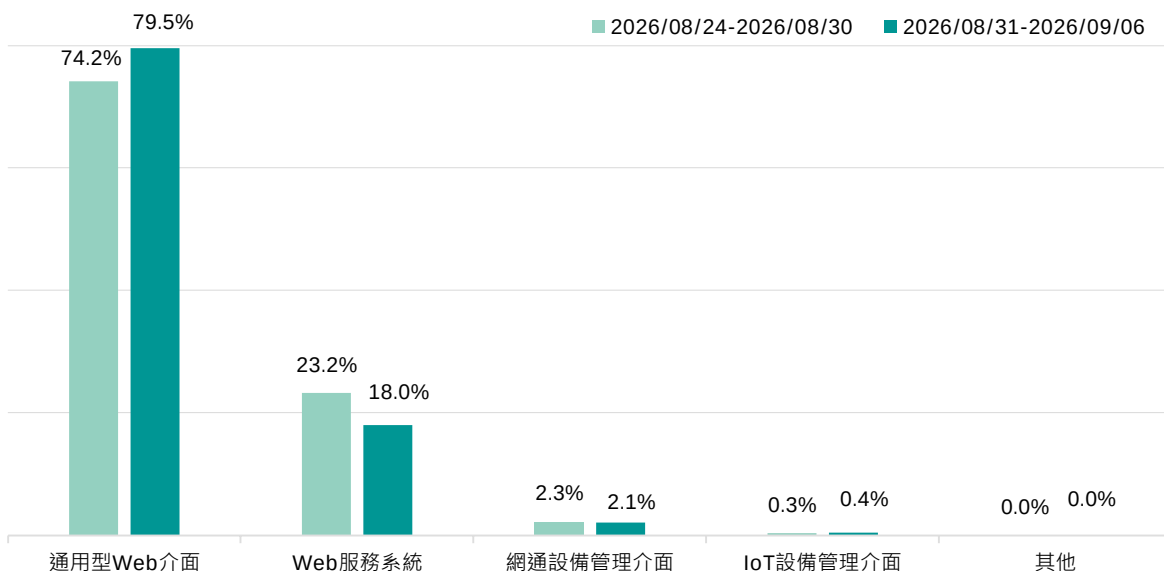


圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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身分驗證繞過漏洞、越界讀取漏洞及指令注入漏洞，攻擊目標涵蓋網站主機伺服器管理系統、程式遞送控制器(ADC&Gateway)、大模型API統一介面與代理伺服器工具、企業級的終端裝置管理與資安防護系統及雲端檔案管理平台。

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	↑1	CVE-2026-41940 ¹	cPanel & WHM	9.8	✓
■	2	↑3	CVE-2026-3055 ²	NetScaler ADC & Gateway	9.8	✓
■	3	↓2	CVE-2026-42271 ³	LiteLLM	8.8	✓
■	4	↑new	CVE-2026-1603 ⁴	Ivanti Endpoint Manager	8.6	✓
■	5	↑new	CVE-2026-2699 ⁵	Progress ShareFile	9.8	

類型 ■ 身分驗證繞過漏洞 ■ 越界讀取漏洞 ■ 指令注入漏洞

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-41940>
2. <https://nvd.nist.gov/vuln/detail/CVE-2026-3055>
3. <https://nvd.nist.gov/vuln/detail/CVE-2026-42271>
4. <https://nvd.nist.gov/vuln/detail/CVE-2026-1603>
5. <https://nvd.nist.gov/vuln/detail/CVE-2026-2699>

■ 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

網站部署應避免將敏感設定檔暴露於公開路徑

本週總計接獲24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異常連線占多數，詳見圖6。本週發現機關網站之 .env 環境設定檔置於網站根目錄，未經授權即可下載。此類檔案主要供網站程式載入執行環境及連線設定，常用於設定資料庫、外部服務或其他系統參數，不應置於可由外部存取的位置。

.env 檔案內容可能涉及帳密、金鑰或服務位址等敏感資訊，建議確認該檔案未置於網站根目錄或其他可由外部直接存取之路徑，並於網站伺服器設定禁止存取 .env、設定檔、備份檔及其他非公開檔案；網站部署或版更時，亦應確認部署套件未將此類檔案一併對外發布。若 .env 已曾對外暴露，應依檔案內容更換可能外洩之資料庫帳密、API Key或其他憑證，並查閱網站存取紀錄及相關系統登入紀錄，確認是否曾遭下載或進一步利用。

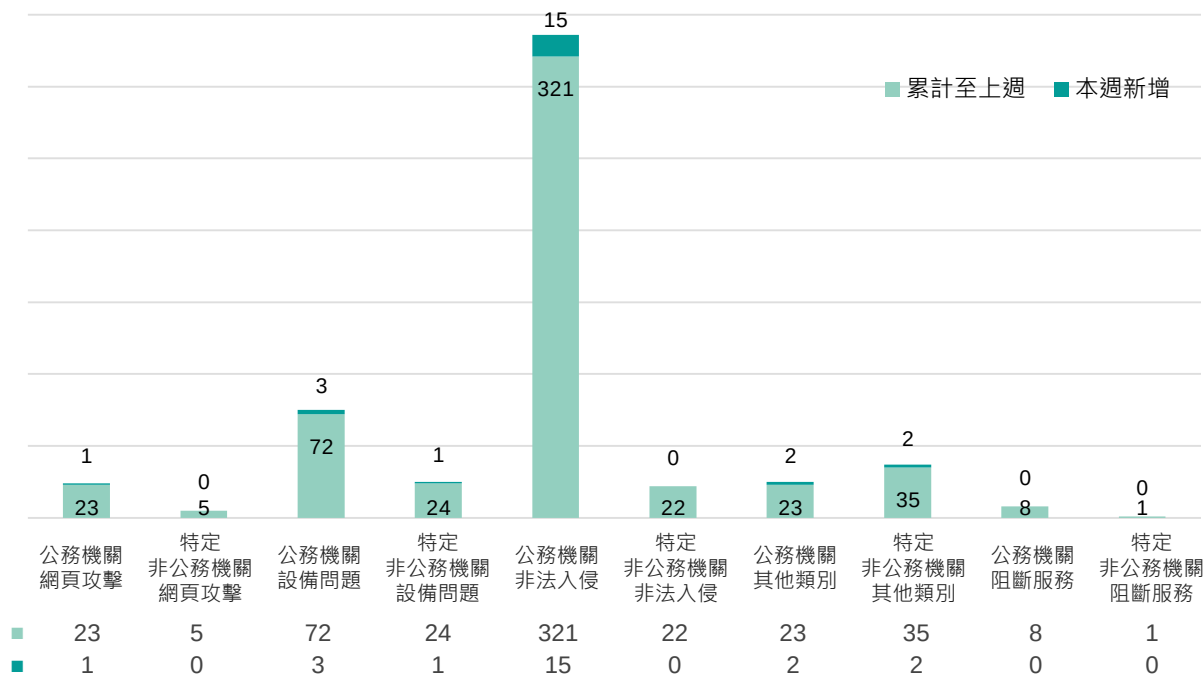


圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

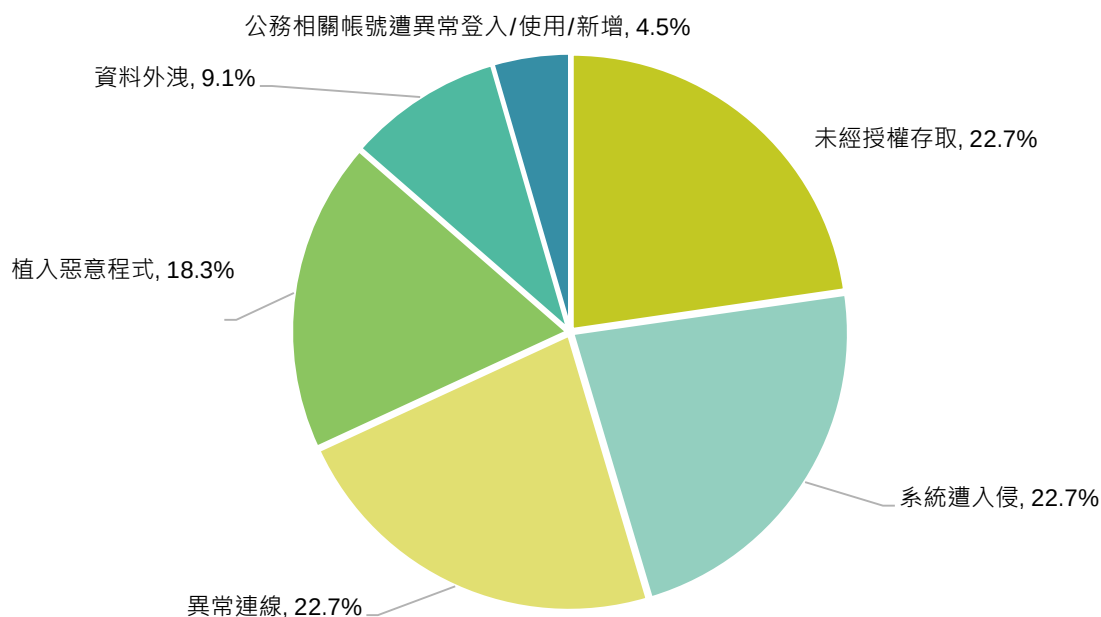


圖6 | 本週公務機關非法入侵事件類型占比

防護建議

除修補漏洞外，應：

以攻擊為出發評估潛在風險

- 攻擊者下載環境設定檔取得帳密與金鑰
- 外洩憑證遭利用進一步存取資料庫與服務

針對潛在風險執行相應改善

- 禁止將.env及敏感設定檔置於網站可直接存取之公開目錄中
- 於網站伺服器設定禁止存取設定檔、備份檔及其他非公開檔案
- 部署與版更前檢查發布內容，避免敏感設定檔誤佈至對外環境
- 若敏感檔案曾外洩，應立即更換帳密、金鑰並查閱相關存取紀錄

3間民間企業揭露重大資安訊息

本週3家民間企業發布重大訊息，產業類別為光電業、半導體業，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
杭特電子股份有限公司	2026年08月31日	杭特公司之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，後續將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。
乾瞻科技股份有限公司	2026年09月01日	乾瞻公司之ERP資訊系統遭受駭客加密攻擊，隨即啟動資安事件應變、防禦及復原機制，並委請外部資訊安全技術專家協同處理。經評估對公司財務、業務及營運皆無重大影響，後續將持續檢視並強化ERP資訊系統與研發資訊環境間之網路分區、存取權限、監控告警、備份復原及其他安全控管機制，以提升整體資通安全防護能力。
創新服務股份有限公司	2026年09月02日	創新服務公司偵測到部份伺服器遭受網路勒索病毒攻擊，致使包含 ERP 在內之部份資訊系統無法正常運作，已立即啟動防禦機制與斷網隔離措施、相關資安應變機制，全面檢視資安系統與加強相關防護。經評估對公司整體營運及財務之影響程度尚不致有重大影響。後續將持續密集監控，並強化網路與資訊基礎架構之管控，以確保資訊系統安全。

■ 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

金融投資與身分冒充回升 產品服務仍占首位

詐騙類型趨勢

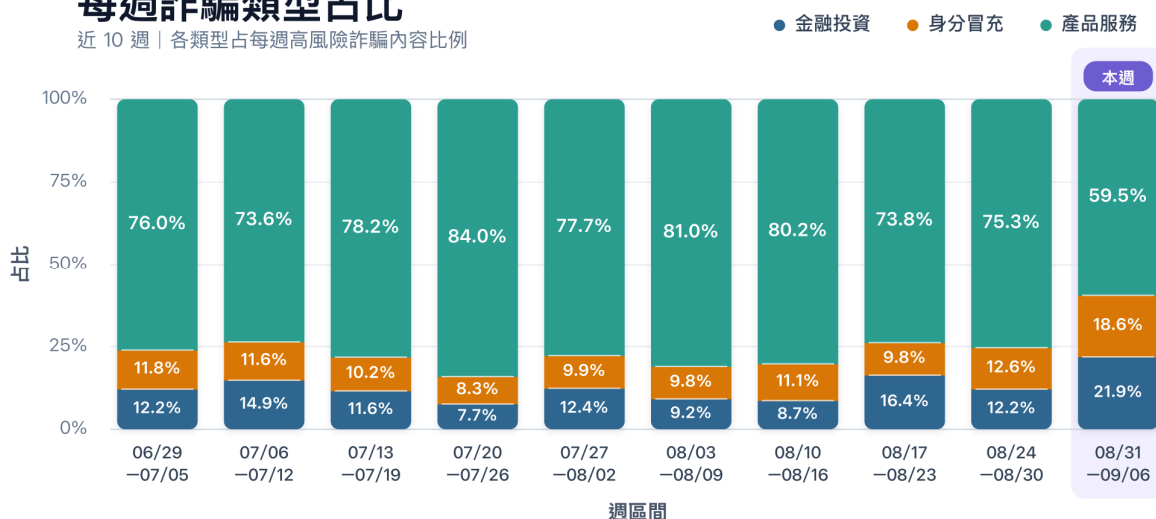
本週金融投資型占比明顯回升，詳見圖7，成為第二大高風險類型，相關內容以資產配置、股票期貨教學及免費觀察名單吸引民眾。這些內容透過講師解說與系統化交易包裝專業形象，再以觀看投資觀點、報名體驗課或私訊領取名單等方式，將民眾的學習需求連結至後續互動。

身分冒充型占比同步回升，相關皮膚保養商品借用機關認證、醫院研發與專家團隊等說法，搭配使用者見證營造可信形象。這些內容再結合免赴院處理的承諾與限時折扣，把專業背書轉為促購訴求，引導民眾點擊購買。

產品服務型占比雖回落，仍居本週首位，防曬美妝、鞋款與旅行收納用品以低價、買一送一及免費換新促購。購車廣告則結合低月付、免頭款與線上下訂折扣，將商品吸引力與付款便利相互搭配，推動民眾下單或聯繫。

每週詐騙類型占比

近 10 週 | 各類型占每週高風險詐騙內容比例



註：各週三類占比合計為 100%；本週以淡色區塊標示。

資料期間：2026/06/29—09/06

圖7 | 每週詐騙類型占比

關鍵字趨勢

「優惠」仍居本週首位，與升至第 9 名的「輕鬆」共同以防曬兼妝前打底、省時便利及限時低價吸引購買，詳見圖 8。「限量」升至第 3 名，搭配購車折扣、低月付及免頭款吸引聯繫；維持第 4 名的「免費」則以鞋款清倉與穿壞換新承諾，結合價格與售後保障訴求促購。

「投資」升至第 2 名，新進本週 Top 10 的「股票」與「市場」分居第 5 名及第 8 名，相關內容以資產管理觀點、財務規劃與交易紀律建立專業形象，再引導觀看或報名免費體驗課。升至第 7 名的「資金」則轉向個人借貸，以快速撥款及專人協助回應週轉需求。

「老師」升至第 6 名，情境由技能教學轉向感情復合與命理服務，以線上解盤與客製化服務引導私訊。「AI」新進第 10 名，則以學員成果、免費學習營及限額贈品招攬創業學習者。本週從商品優惠、投資學習到生活改善，各類訴求分別透過下單、報名或私訊，將民眾的不同需求帶入後續互動流程。

詐騙關鍵字占比週比變化

以本週為主 | 完整顯示本週 Top 10

○ 前週 8/24-8/30 ● 本週 8/31-9/6

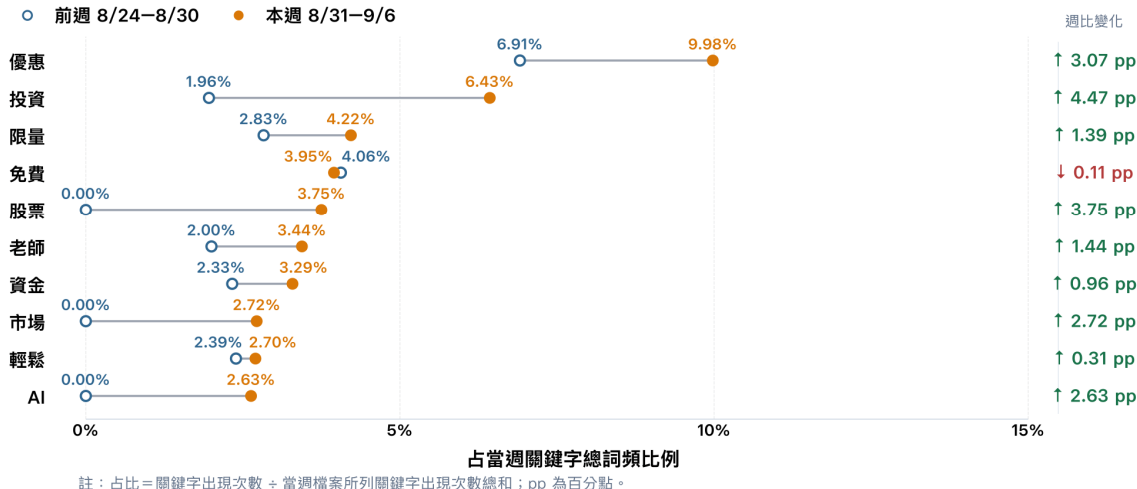


圖 8 | 詐騙關鍵字占比週比變化

焦點文章

從賽事經驗建構台灣資安人才生態圈的實踐 競賽基因的傳承與世代交替的思考

序章：競賽基因的傳承與世代交替的思考

自 2014 年臺灣戰隊於世界駭客大會 (DEF CON Capture The Flag, CTF) 奪亞以來，競賽即成為國內資安人才領域不可或缺的育才搖籃。近十年間，無數自賽事淬煉而出的選手，已成為我國關鍵基礎設施、資安產業和高科技製造業的中流砥柱。

2023 年，國家資通安全研究院 (下稱本院) 人才培力中心組成後勤團隊，協助臺灣聯隊 (TWN 48) 遠征拉斯維加斯，於第 31 屆 DEFCON CTF 決賽再創全球第三佳績。本院觀察到，國內戰隊首度導入「戰隊經理人 (PM) 」制度，專責評估與分工，有效緩解跨隊伍整合的適應問題，並激發更多創意思維。

然而，隨著成熟選手邁入職場，世代交替帶來新血斷層問題。如何向下扎根、擴大參與基數，讓資安學習大眾化與在地化，成為人才培育的核心課題。

實踐：構建「CTF 資安人才培育生態圈」

1. 雙軌化策略：打造資安高手的進階賽場與新手引路

為突破單向教學限制、模擬賽間高度心流的解題情境，本院自 2023 年底起草「CTF 種子生態圈定義與分布」初稿並採雙軌聚焦以辦理系列工作坊，詳見圖9。

針對進階學員，深化中高難度題型與 CVE 漏洞復現；針對新手師生，以軟性經驗交流、解題心法教學為主，輔以提高團隊跨校組隊增進跨校互動經驗並協助教師掌握學習上的資源缺口，強化師長成為隊伍信心支柱的重要角色。

2. 沉浸式演練：軟硬體安全思維與手感鍛鍊

培育活動不只停留在理論講授，更融入了多元的 CTF 賽事模擬演練，誘發學員在有限時間內建立起臨場應變的敏銳度。

培訓融入了 CTFd 平台演練與手動實作，訓練學員強化 Jeopardy 題型掌握外，亦跨域建立

焦點文章



圖9 | CTF 種子生態圈定義與分布

韌體分析與硬體安全防禦思維，累積實務手感與行為觀察決策能力。此類演練促成跨校社群切磋，將課本知識化為真實守護能量。

3. 沙龍進化與跨代共鳴：產學研的對話平台

人才培育的終點，非僅止於競賽，更在於將熱情轉化為職場即戰力。本系列的招牌議程為「跨界沙龍座談」，詳見圖10，亦邀請產學專家與選手對話，解答新手焦慮：

Q1：如何面對資訊淹沒與工具依賴？

A1：新手不必急著幫自己貼上標籤或盲目追趕所有熱點。打好網路架構與底層程式的基本功，具備正確資訊識讀，才是無法被取代的核心護城河。

Q2：強者與新手該如何達成良好的團隊協作？

A2：好的戰隊需要良好的管理與任務拆解，新手可以從熟悉賽制、選擇自己有興趣的單一領域鑽研開始；強者則需學會引導與分工，讓每位成員都能在實務中找到定位，避免出現孤立感。

焦點文章

Q3：如何有意識地提升職涯與價值的選擇？

A3：玩 CTF 不單是為了比賽，更是絕佳覺察個人特質、累積強項以解決未知問題的抗壓能力的管道。在資安領域中，保有持續探索的好奇心、人際社群的信任連結以及面對挫折時的修復力，皆是未來跨入產業極具價值的無形資產。



圖10 | 沙龍座談實景

轉型：AI 時代下的資安思維與「人機協作」新定義

因應生成式 AI 普及，本院首度將「AI 鏈結」列為培訓主軸，傳遞核心方針：

「AI 改變的是解題與分析的速度，但沒有改變下判斷的責任歸屬；工具會改變，題型會改變，但資安的本質不會改變——這個本質，就是在不確定的情境中，做出『最恰當判斷與即時應變』的能力。」

優秀專家能將 AI 發揮極致，關鍵在於具備底層知識以建構精準環境、拆解任務並監督 AI 是否產生幻覺與誤導。人類在「戰略指揮、直覺驗證與責任承擔」上的價值不可替代，本院期許引導學員晉升為「人機協作指揮官」。

焦點文章

■ 展望：扎根校園，鏈結產學無縫接軌

截至 2026 年 7 月，培訓活動已獲全台 90 所校系響應（大專 56 所、高中職 34 所），累計逾 350 人次參與。回饋顯示，活動大幅提升自主組隊意願，亦有許多教師規劃將實戰經驗帶回校園或親自帶隊，展現教學相長的正向循環。

資安防線建構是一場馬拉松。未來本院將持續扮演產學研橋樑，推動扎實培育機制，與師生共同築起堅韌且具信任度的國家資安防線。

關鍵字：CTF 競賽、資安人才培育、世代傳承

刊 名 資安週報第 61 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