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
檔案上傳應落實伺服器端驗證 避免前端限制遭繞過

聯防監控
防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕
企業級網路防火牆軟體仍為攻擊熱點

重大漏洞
Microsoft與SonicWall高風險漏洞應盡速修補

外部曝險分析
整體風險漏洞略減 未部署WAF明顯增加

實兵演練
實兵演練揭露設備版本未更新風險 已知漏洞恐遭利用

網路巡查高風險詐騙
健康、投資與私密商品廣告風險升溫

焦點文章
115上半年政府領域資安事件趨勢研析

2026.07.23
054

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

檔案上傳應落實伺服器端驗證 避免前端限制遭繞過

本週總計接獲16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。 本週有機關遭駭客利用網站檔案上傳功能植入網頁木馬取得網站設定檔(Web.config)，後續並透過網站服務程序執行系統指令，蒐集內部網路環境資訊。

由於前端檢核係於使用者瀏覽器中執行，上傳檔案之名稱、格式及請求內容均可能遭竄改；如伺服器端未重新驗證，即可能使惡意檔案繞過限制並遭上傳執行。建議檔案上傳功能除於前端提示允許格式外，伺服器端仍應依業務需求重新檢查副檔名、檔案內容、大小及格式，並將上傳檔案存放於不可執行之位置，避免前端檢核遭繞過後形成網頁木馬植入風險。

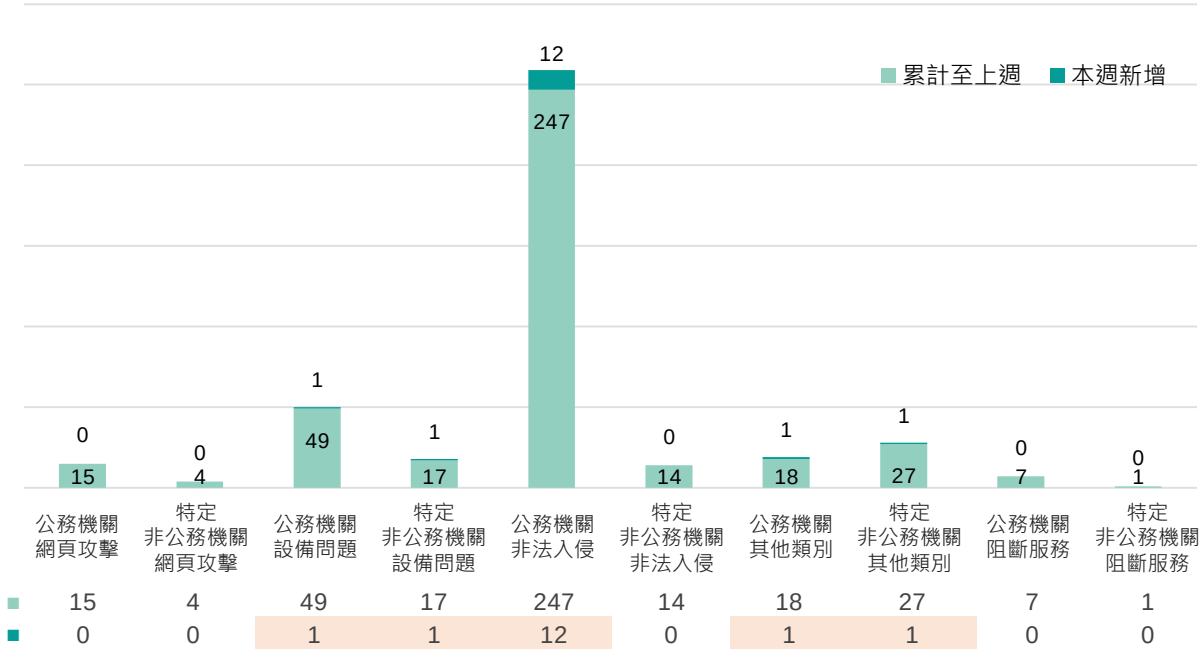

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

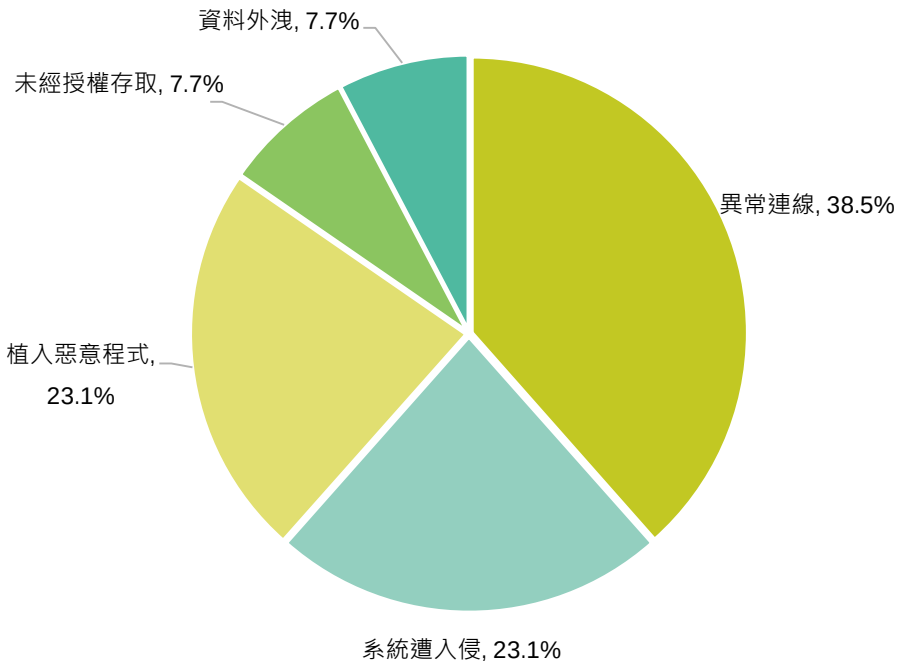

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者上傳網頁木馬取得網站控制權 ➢ 利用網站程序執行系統指令橫向滲透	➢ 伺服器端重新驗證檔案格式、內容及大小，防止惡意檔案繞過前端檢查 ➢ 上傳檔案存放於不可執行目錄，避免遭植入網頁木馬執行惡意程式 ➢ 限制網站服務帳號權限，避免遭利用執行系統指令或存取敏感檔案 ➢ 導入網站應用程式防火牆與日誌監控，即時偵測異常上傳及指令執行行為

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，產業類別為電子零組件業，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
松上電子股份有限公司	115年7月17日	松上公司使用之部分資訊系統遭駭客網路攻擊，資訊部門發現網路異常後，已立即啟動相關防禦機制與進行復原，目前受影響之系統已恢復正常運作。 經評估對公司營運無重大影響，後續仍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。

■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15.5%，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12.9%，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、以及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。

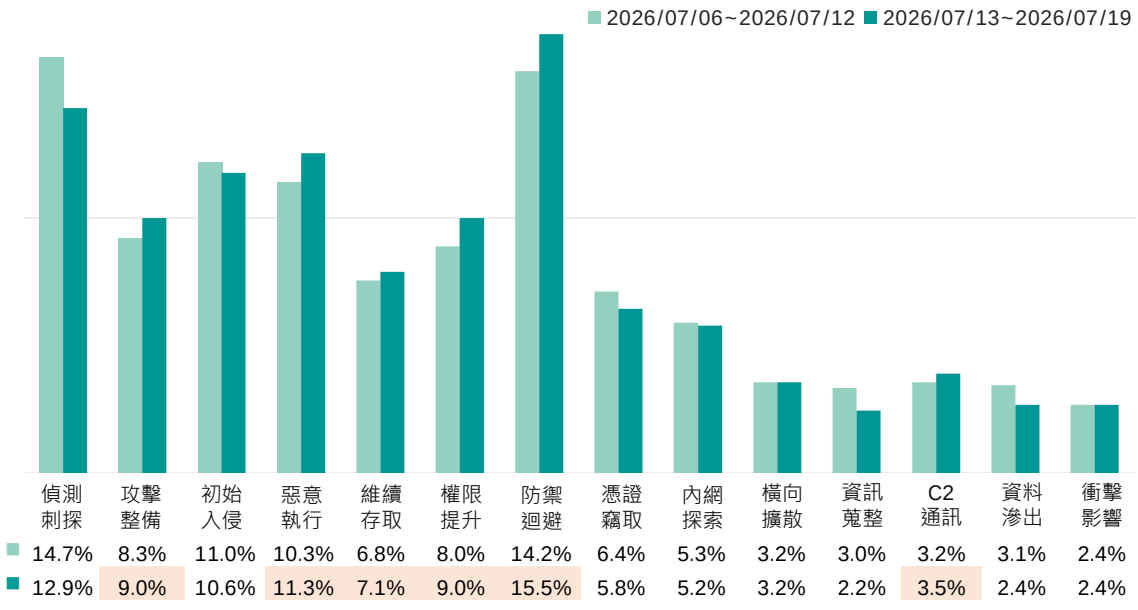

圖3 | 資安聯防監控攻擊階段統計

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，監控異常行為
- 保留並稽核 PowerShell、Cmd 等指令執行紀錄
- 限制或控管 LOLBins（合法系統工具）及高風險工具使用
- 落實最小權限原則，強化特權帳號管理與多因素驗證（MFA）
- 建立檔案、服務及安全性設定異常變更告警機制

偵測刺探(Reconnaissance)

- 監控異常掃描流量、連線探測及帳號探測行為
- 定期盤點並降低對外暴露資產與服務
- 關閉不必要的服務與連接埠，落實系統修補
- 結合威脅情資，封鎖已知惡意來源 IP 或網段
- 建立掃描事件告警與分析機制，及早發現攻擊前期活動

■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

企業級網路防火牆軟體仍為攻擊熱點

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78.64%、「遠端控制」服務攻擊占比17.88%，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73.71%。「遠端控制」服務亦有22.96% 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React Server Component存在遠端程式碼執行漏洞之CVE-2025-55182，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。

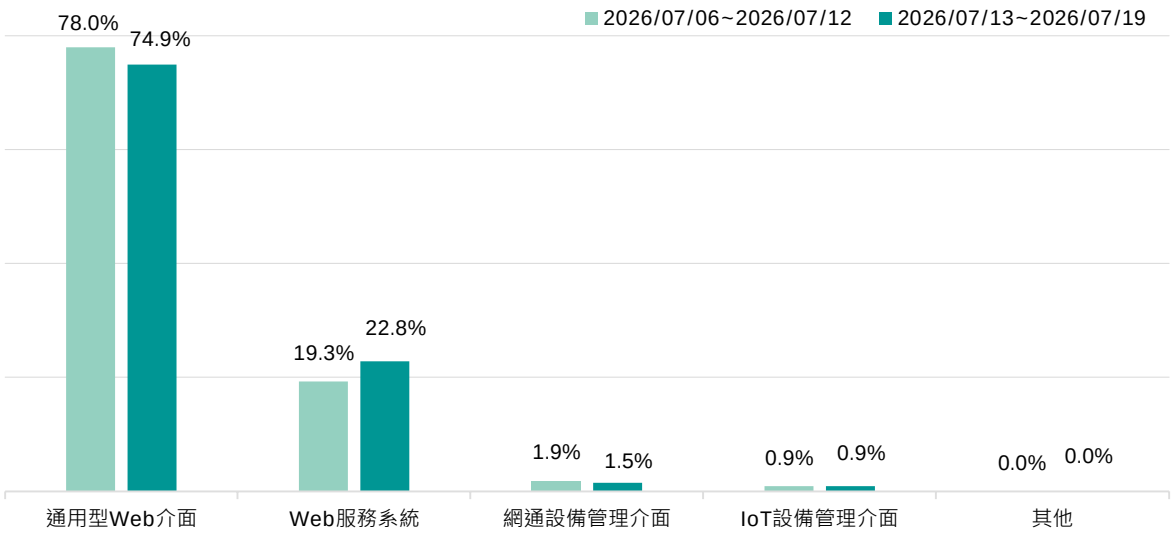

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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授權缺失漏洞、遠端程式碼執行漏洞、跨站請求偽造、資訊外洩漏洞及路徑遍歷漏洞，攻擊目標涵蓋企業級網路防火牆軟體、前端框架之伺服器端元件架構、多選下拉選單元件、開源後端伺服器框架及內容管理系統之網站優化外掛程式。

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-2025-20362[1]	Cisco Secure ASA & FTD	6.5
■	2	⬆New	CVE-2025-55182[2]	React Server Components	10
■	3	-	CVE-2025-47204[3]	Bootstrap Multiselect	6.1
■	4	-	CVE-2025-53364[4]	Parse Server	5.3
■	5	-	CVE-2025-30567[5]	WordPress WP01	7.5

類型 ■ 授權缺失漏洞 ■ 遠端程式碼執行漏洞 ■ 跨站請求偽造 ■ 資訊外洩漏洞 ■ 路徑遍歷漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
2. https://nvd.nist.gov/vuln/detail/CVE-2025-55182
3. https://nvd.nist.gov/vuln/detail/CVE-2025-47204
4. https://nvd.nist.gov/vuln/detail/CVE-2025-53364
5. https://nvd.nist.gov/vuln/detail/CVE-2025-30567

■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SonicWall高風險漏洞應盡速修補

- 微軟釋出115年7月份安全性更新，共修補包含Active Directory Federation Services、Microsoft Office SharePoint及Windows Kernel等共628個漏洞[1]，其中包含76個高風險漏洞，且CVE-2026-56155、CVE-2026-56164及CVE-2026-58644漏洞已遭駭客利用。

- SonicWall SMA 1000系列存在多項高風險安全漏洞(CVE-2026-15409與CVE-2026-15410)[2]，類型分別為伺服器端請求偽造(Server-Side Request Forgery)與程式碼注入(Code Injection)。兩項漏洞皆已遭到駭客利用，請儘速確認並進行修補。

1. https://msrc.microsoft.com/update-guide/releaseNote/2026-Jul
2. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008

■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

整體風險漏洞略減 未部署WAF明顯增加

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2,917項。其中，「元件高風險漏洞」以941項居首，「過時或弱加密協定」840項次之，「TLS憑證不受信任」609項位居第三。前三項合計2,390項，占前10大風險項目總數約81.9%，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2,954項，整體風險數量減少37項，降幅約1.3%，詳見圖5。

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957項微降至941項，降幅約1.7%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍較為集中；本期Archive_Tar相關弱點(CVE-2020-28949)已見減少，惟新增Archive_Tar相關弱點(CVE-2020-36193)，後續仍須持續關注相關元件版本與修補情形。「TLS憑證不受信任」由614項微降至609項，降幅約0.8%；「過時或弱加密協定」由852項微降至840項，降幅約1.4%。另在網站防護設定方面，「CSP設定不當」由255項微增至256項，增幅約0.4%；「未部署WAF」由114項增至145項，增幅約27.2%。整體而言，本期外部曝險程度小幅下降，各項目呈現小幅下降，惟未部署WAF上升幅度較大，顯示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。

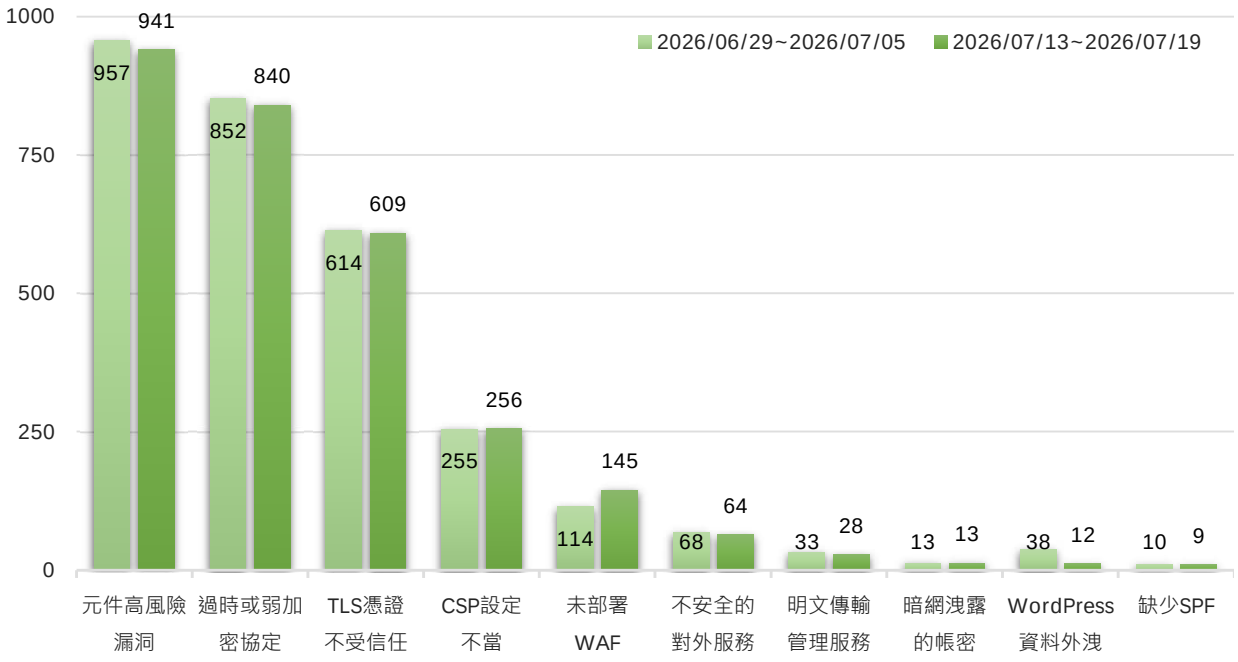

圖5 | EASM檢測結果統計(前10大風險)

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

■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

實兵演練揭露設備版本未更新風險 已知漏洞恐遭利用

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7/17止已累計226筆攻擊紀錄，本週新增弱點數量共13筆，分別為「驗證機制失效」3筆、「無效的存取控管」3筆、「軟體供應鏈失效」3筆、「注入攻擊」2筆及「加密機制失效」2筆，詳見圖6。

本週演練發現，衝擊性較高之弱點為「軟體供應鏈失效」。攻擊者利用弱點掃描工具進行檢測，發現目標設備使用之作業系統版本存在已知安全漏洞，包括CVSS 10.0 Critical與CVSS 4.0 Low之漏洞。針對CVSS 10.0 Critical漏洞，攻擊者利用公開漏洞利用程式進行測試，成功於目標設備建立測試檔案，並透過瀏覽器存取該路徑確認檔案已成功建立，顯示攻擊者可利用該漏洞執行未授權操作。另針對CVSS 4.0 Low漏洞，攻擊者利用公開漏洞利用程式於設備服務介面進行測試，成功觸發跨網站腳本攻擊(Cross-Site Scripting, XSS)，確認目標設備存在XSS弱點，可能遭攻擊者利用建立惡意連結，誘導使用者執行非預期腳本，增加帳號資訊外洩或社交工程攻擊之風險。

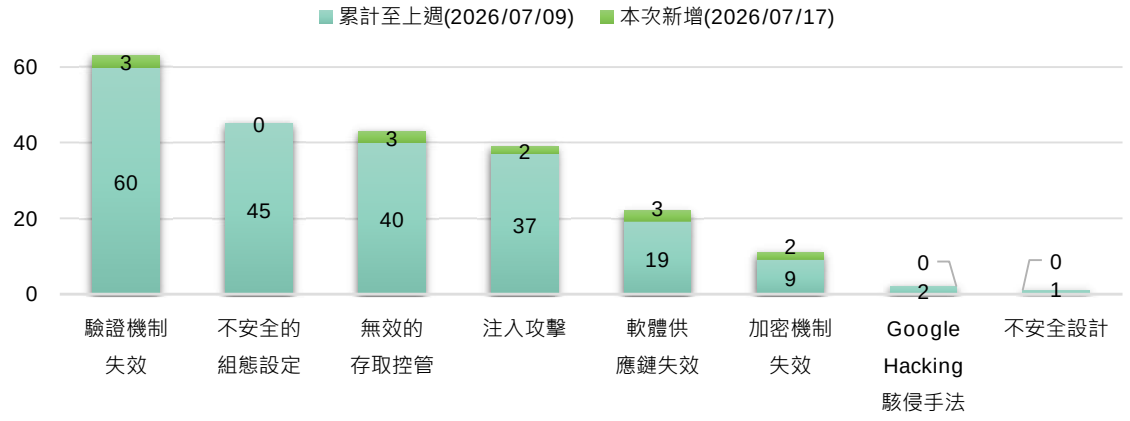

圖6 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應定期盤點設備使用之作業系統與元件版本，持續追蹤原廠安全公告並進行更新，以降低已知漏洞風險
- 如因業務需求無法立即完成修補，應依原廠建議採取緩解措施，例如限制管理介面與服務介面之存取來源，降低設備暴露於外部網路之風險
- 針對對外提供服務之Web介面，應強化輸入驗證與安全設定，避免跨網站腳本攻擊(XSS)等應用層漏洞遭利用，並建立異常行為監控機制，以降低攻擊風險

■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

健康、投資與私密商品廣告風險升溫

本週高風險廣告以「優惠」、「健康」及「免費」等話術最為突出，並結合醫療功效、投資資訊、開運祈福及不明商品銷售，誘導民眾私訊、加入LINE或點擊陌生網站，詳見圖7。

免費體驗包裝健康奇效

護眼、潤喉、男性保健、漏尿改善及養肝商品，常以「醫師推薦」、「短期見效」、「免費體驗」及「限量名額」吸引民眾。部分廣告甚至宣稱可快速改善視力、脫敏修復或使白髮轉黑。

健康食品及一般商品不能取代醫療行為。遇到快速見效、專業人士背書或免費試用廣告，應查證許可證、成分標示及代言真實性。

免費問事與宗教商品引導加LINE

免費運勢解析、轉運祈福及開運手鍊等廣告，常透過每日限量、留言登記或加入LINE製造急迫感，再推銷付費服務或商品。

宗教信仰及命理服務不能保證改運、招財或消災。切勿因免費名額而提供生日、住址、證件或金融資料。

投資與AI資訊以免費加入導流

ETF配息表、投資懶人包、AI推薦系統及免費電子報，常要求民眾點擊加入討論區或領取資料。此類內容可能先提供免費資訊建立信任，再引導加入假投資群組或不明平台。

投資前應透過合法金融機構查證，不聽從陌生網友指示匯款、儲值或下載投資程式。

私密影音隨身碟藏有資安風險

部分廣告販售所謂高畫質影音合集隨身碟，強調無刪減、雲端更新及快遞單不顯示敏感詞，並導向名稱不明的購物網站。

來源不明的隨身碟可能含有惡意程式、侵權內容或偽造容量。切勿任意插入電腦或手機，也不要向不明網站付款。

貸款、分期及兼職廣告蒐集個資

資金週轉、無卡分期購買手機、遠端兼職及遊戲代儲等內容，常要求透過LINE私訊，並提供身分證件或付款資料。

合法貸款及分期仍會進行信用審核。切勿寄送提款卡、提供驗證碼、網路銀行密碼或依指示操作ATM。

本週防詐提醒

1. 免費體驗、限量名額及立即領取，都是常見催促話術。
2. 健康商品宣稱快速見效或專業推薦，應查證許可與來源。
3. 不加入陌生投資群組或下載不明投資程式。
4. 不購買來源不明的影音隨身碟或私密商品。
5. 不向陌生客服提供證件、帳戶、提款卡及驗證碼。

綜合觀察

本週高風險廣告多採取「免費優惠吸引—點擊或私訊導流—加入LINE或陌生網站—要求付款或提供資料」的模式。

凡遇到誇大功效、保證獲利、名額有限或要求脫離原平台交易的廣告，應立即停止操作並撥打165查證。

圖7 | 詐騙關鍵字文字雲

焦點文章

115上半年政府領域資安事件趨勢研析

可預期風險持續發生，落實基本控制為治理重點

115年上半年可識別之事件發生原因中，以使用或下載來源不明之應用程式或套件、應用程式漏洞及設備異常或毀損最為常見；弱密碼、網站設計不當及作業系統漏洞亦持續出現。整體觀察，多數事件並非源自高度複雜或全新攻擊手法，而是既有風險在不同系統、設備及使用情境中反覆遭到利用。

一、攻擊手法未必複雜，可預期風險仍為主要入口

上半年持續發現使用者遭搜尋引擎導向偽冒網站，下載並執行夾帶惡意程式之安裝檔；另有攻擊者利用既有應用程式漏洞、弱密碼及網站安全設計缺口取得系統權限。相關風險已有明確防護方式，宜透過限制未核准軟體安裝、提供可信任軟體來源、由系統端限制弱密碼，以及持續追蹤對外系統與第三方元件弱點，降低相同問題反覆形成事件之可能。

二、聯網設備安全設定、韌體更新及支援期限管理仍待強化

上半年亦發現無線分享器、監視器及門禁刷卡機等聯網設備遭植入惡意程式或利用。實務上，部分設備未變更預設帳密、未限制管理介面存取，亦缺乏網路區隔及韌體更新；另有設備已屆原廠停止支援（End of Support, EOS），無法再取得安全性更新。建議將聯網設備納入資產及弱點管理，掌握安全設定、韌體版本、已知弱點及支援期限，並針對已停止支援且缺乏有效補償措施之設備，依風險規劃汰換。

三、服務恢復後，仍須確認事件原因與影響範圍

「無法確認事件原因」為上半年件數最高之項目，部分涉及監視器、門禁設備、防火牆或交換器。此類設備常因日誌不足，或於異常後立即重啟、重置及汰換，致事後難以釐清入侵途徑及影響範圍。事件處置除恢復服務外，仍應確認設備之網路連線、管理帳號、關聯系統及同型設備是否受影響，並於處置前保存必要日誌、設定及診斷資訊。

結語

上半年事件顯示，降低可預期風險仍是現階段治理重點。後續宜同步強化可信軟體管理、既有弱點修補及聯網設備生命週期管理，並提升事件原因與影響範圍之辨識能力，使服務恢復與風險排除得以並行。

關鍵字：可預期風險、聯網設備治理、日誌保存

刊　　名　資安週報第 54 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