



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

整體曝險風險呈下降趨勢 元件高風險漏洞降幅較明顯

重大漏洞

Cisco與Citrix高風險漏洞應盡速修補

實兵演練

實兵演練揭露驗證機制失效 致弱密碼遭利用與主機權限提升風險

聯防監控

初始入侵高居首位 防禦迴避仍具威脅

蜜罐誘捕

AI應用套件及企業級終端裝置管理與資安防護系統成攻擊熱點

事件通報

強化 API 身分驗證與存取控管 降低未授權存取風險

網路巡查高風險詐騙

權威健康話術回升 翡翠團購與私訊導流升溫

焦點文章

資安情資分享與威脅趨勢報告

2026.09.03

060

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

整體曝險風險呈下降趨勢 元件高風險漏洞降幅較明顯

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2,803項。其中，「元件高風險漏洞」以884項居首，「過時或弱加密協定」807項次之，「TLS憑證不受信任」603項位居第三。前三項合計2,294項，占前10大風險項目總數約81.8%，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2,864項，本期整體風險數量減少61項，降幅約2.1%，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931項減至本期884項，降幅約5.0%。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。本期另檢測出Drupal檔案上傳處理相關弱點(CVE-2020-13671)，因Drupal Core未妥善處理特定上傳檔案名稱，可能導致檔案副檔名及MIME類型判斷錯誤，並於特定主機環境設定下使惡意檔案被當作PHP程式執行，造成遠端程式碼執行風險。考量Drupal 7、8及9系列版本均已終止官方安全支援，建議升級至仍受官方安全維護之Drupal版本，並套用最新安全修補版本，以持續取得官方安全更新。「過時或弱加密協定」由831項減至807項，降幅約2.9%；「TLS憑證不受信任」由589項增至603項，增幅約2.4%。另「CSP設定不當」由247項減至239項，降幅約3.2%；「未部署WAF」由125項減至121項，降幅約3.2%。

整體而言，本期外部曝險風險呈下降趨勢，其中「元件高風險漏洞」降幅較為明顯，「過時或弱加密協定」、「CSP設定不當」及「未部署WAF」亦呈下降；惟「TLS憑證不受信任」較上期增加，顯示憑證有效性及信任鏈設定仍有改善空間，建議持續強化元件漏洞修補、加密通訊及憑證管理，以降低相關曝險風險。

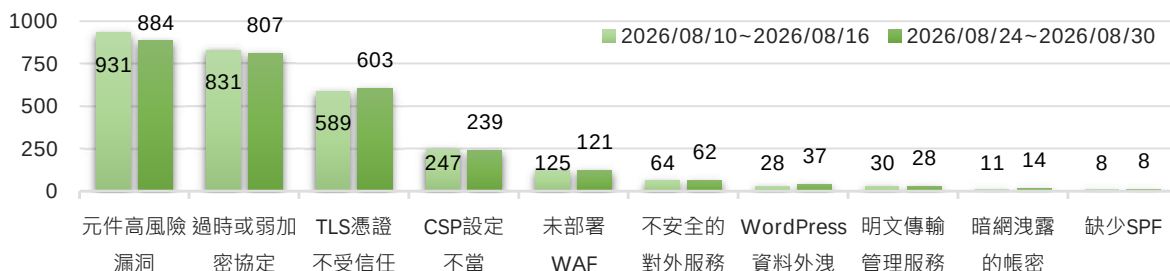


圖1 | EASM檢測結果統計(前10大風險)

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

Cisco與Citrix高風險漏洞應盡速修補

- Cisco Secure Workload 存在 4 項高風險安全漏洞(CVE-2026-20231、CVE-2026-20315、CVE-2026-20317及CVE-2026-20318)¹，類型分別為注入(Injection)、不當存取控制(Improper Access Control)、不當驗證(Improper Authentication)及不當輸入驗證(Improper Input Validation)。未經身分鑑別或已通過身分鑑別之遠端攻擊者可利用該等漏洞，造成系統機密性、完整性或可用性受影響。
- NetScaler ADC與NetScaler Gateway存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-19490)²，當設備設定為Gateway(SSL VPN、ICA Proxy、CVPN或RDP Proxy)或AAA虛擬伺服器時，未經身分鑑別之遠端攻擊者可藉由替代路徑繞過身分鑑別機制。

1. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-csw1-shSvndWP>
2. <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939>

■ 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失效 致弱密碼遭利用與主機權限提升風險

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8/28止已累計306筆攻擊紀錄，本週新增弱點數量共17筆，分別為「不安全的組態設定」6筆、「驗證機制失效」5筆、「無效的存取控管」3筆、「注入攻擊」2筆及「加密機制失效」1筆，詳見圖2。

本週演練發現，衝擊性較高之弱點為「驗證機制失效」。攻擊者透過FFUF工具掃描目標網站目錄，發現「/admin」登入介面，進一步嘗試進行帳號密碼猜測，並使用常見管理者帳號搭配弱密碼成功登入系統。登入後攻擊者利用系統既有之檔案上傳功能，上傳Reverse Shell PHP後門程式，確認系統可直接執行上傳之PHP程式。攻擊者透過該程式與監聽端建立Reverse Shell連線，成功取得「www-data」服務帳號之Shell存取權限，後續利用目標主機存在之CVE-2026-31431漏洞，執行公開漏洞利用程式進行權限提升，成功取得Root權限。

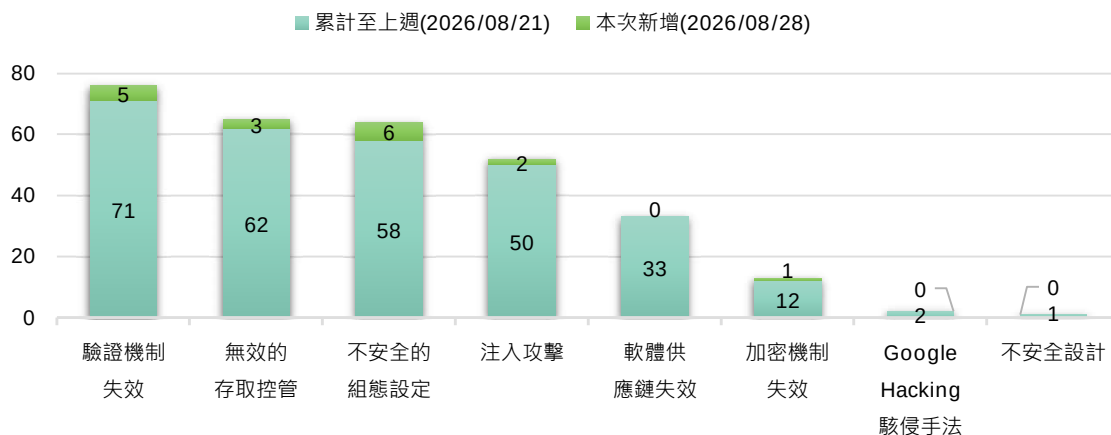


圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應禁止使用預設帳號與常見弱密碼，建立高強度密碼政策，並限制登入失敗次數，以降低帳號遭密碼猜測之風險
- 檔案上傳功能應於伺服器端進行檔案類型與內容驗證，並限制上傳目錄之程式執行權限，避免上傳惡意程式遭執行
- 管理介面應限制來源IP或網段，避免直接暴露於外部網路，必要時搭配VPN或多因素驗證(MFA)

■ 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

■ 初始入侵高居首位 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。「初始入侵」為最常見攻擊手法，占比12.9%，顯示攻擊者持續透過對外系統弱點及軟體供應鏈等管道尋求進入目標環境的機會。觀察到的主要手法包括利用對外應用程式漏洞、入侵軟體供應鏈、以及入侵軟體相依套件與開發工具。攻擊者可能利用未修補的對外應用服務漏洞直接取得初始存取權限，亦可能透過入侵軟體供應商、第三方元件、相依套件或開發工具，將惡意內容植入正常軟體或更新流程，藉由既有信任關係滲透目標環境。此類攻擊除具高度隱蔽性外，亦可能同時影響多個使用相同軟體或元件的組織，增加事件影響範圍與追查難度。建議機關持續落實對外系統弱點掃描與修補，強化第三方軟體及供應商資安風險管理，並建立軟體來源、相依套件及更新機制的完整性驗證，以降低攻擊者利用系統弱點或供應鏈管道取得初始存取權限的風險。

「防禦迴避」事件本週占比為12.5%，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及清除活動痕跡等方式，降低惡意行為遭安全機制偵測的可能性。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機制，降低系統對操作行為的可追溯性，並藉由合法程序或其他系統元件間接執行指令，以規避傳統偵測規則；部分活動亦會在完成操作後清除 Shell 或系統指令歷程，以隱藏攻擊軌跡並增加事後鑑識難度。此類行為具有高度隱蔽性，可能影響資安監控與事件調查的完整性。

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行為建立偵測機制，以降低攻擊者規避防禦與隱匿活動的風險。

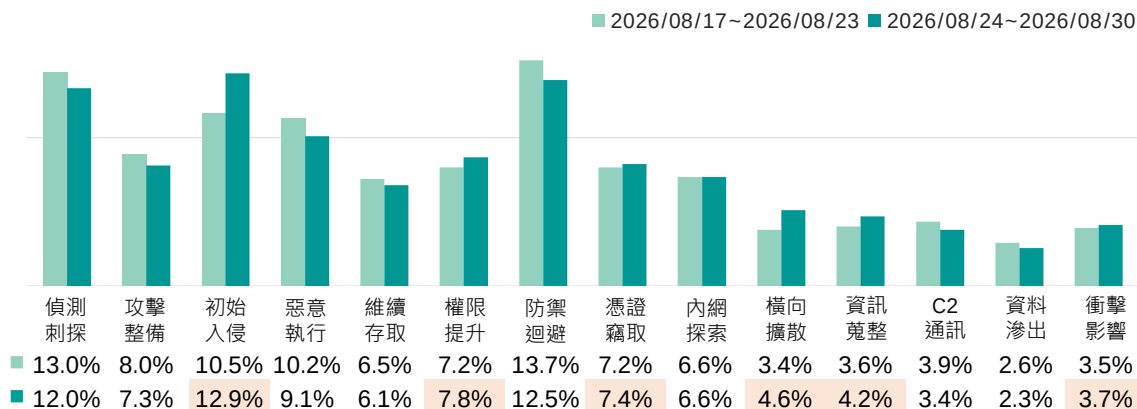


圖3 | 資安聯防監控攻擊階段統計



防護建議

建議機關採取下列防護措施



初始入侵 (Initial Access)



定期執行對外系統弱點掃描，並優先修補高風險及已知遭利用漏洞



強化第三方軟體、供應商及軟體供應鏈之資安風險管理



建立軟體來源、相依套件及開發工具之安全性檢核機制



驗證軟體與更新套件的完整性及來源可信度，避免遭植入惡意內容



持續盤點對外服務及暴露面，降低非必要服務遭攻擊利用的風險



防禦迴避 (Defense Evasion)



加強監控指令執行、指令歷程停用、修改或清除等異常行為



落實系統及安全日誌集中保存，並建立日誌完整性保護機制



針對異常程序鏈、合法工具遭濫用及間接指令執行建立偵測規則



限制非必要的系統管理工具及高權限指令使用，落實最小權限原則



定期檢視端點偵測與日誌告警機制，提升攻擊軌跡保存及事件鑑識能力

■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應用套件及企業級終端裝置管理與資安防護系統成攻擊熱點

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76.86%、「遠端控制」服務攻擊占比19.49%，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74.12%。「遠端控制」服務亦有21.72%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Cisco Secure ASA & FTD軟體存在授權缺失漏洞之CVE-2025-20362，遭攻擊次數增加導致。

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。

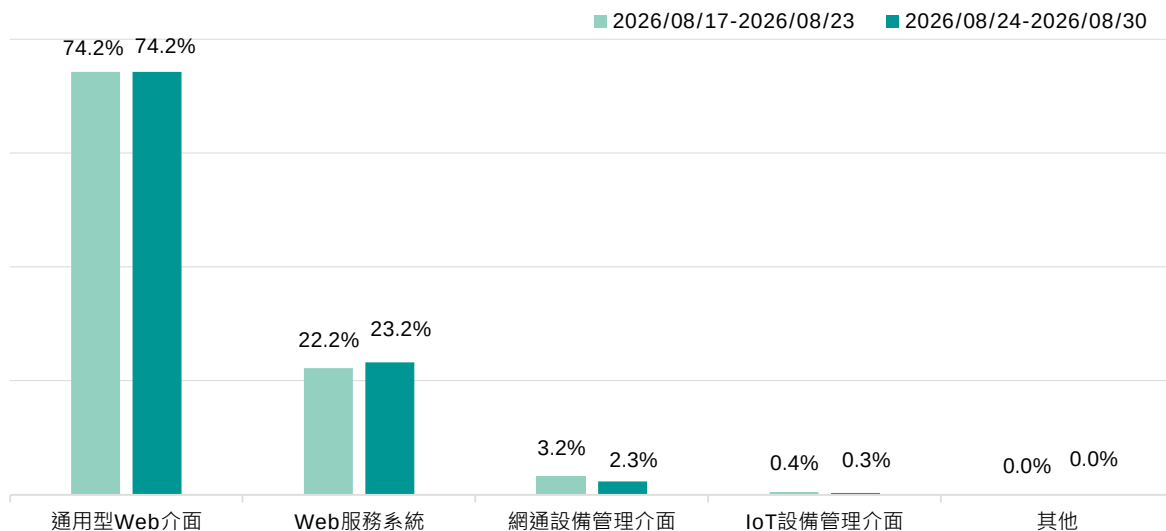


圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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

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	-	CVE-2026-42271 ¹	LiteLLM	8.8	✓
■	2	-	CVE-2026-41940 ²	cPanel & WHM	9.8	✓
■	3	↑ new	CVE-2026-1281 ³	Ivanti Endpoint Manager Mobile	9.8	✓
■	4	↑ new	CVE-2026-1340 ⁴	Ivanti Endpoint Manager Mobile	9.8	✓
■	5	↓ 2	CVE-2026-3055 ⁵	NetScaler ADC & Gateway	9.8	✓

類型 ■ 指令注入漏洞 ■ 身分驗證繞過漏洞 ■ 程式碼注入漏洞
 ■ 越界讀取漏洞

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-42271>

2. <https://nvd.nist.gov/vuln/detail/CVE-2026-41940>

3. <https://nvd.nist.gov/vuln/detail/CVE-2026-1281>

4. <https://nvd.nist.gov/vuln/detail/CVE-2026-1340>

5. <https://nvd.nist.gov/vuln/detail/CVE-2026-3055>

■ 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

強化 API 身分驗證與存取控管 降低未授權存取風險

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。本週發現機關網站部分API於使用者未登入狀態下，即可直接呼叫並取得系統資料，且測試及正式環境均存在相同情形，攻擊者僅送出空白JSON內容，未提供帳號、Token或查詢條件，系統仍回傳資料，顯示相關API可能未妥善限制未登入使用者存取，對空白或缺少必要參數之請求亦未適當拒絕。

API路徑、請求方法及參數格式可透過前端程式、正常操作所產生的網路請求，或Swagger/OpenAPI等文件被掌握，攻擊者可據此重現API請求，因此後端仍須逐次確認使用者身分、存取權限及請求內容。涉及非公開或敏感資料之API，應在每次請求確認使用者身分及資料存取權限；對未提供必要參數、空白內容或格式異常之請求，亦應依預期規則拒絕處理，降低未登入使用者透過直接呼叫API取得系統資料之風險。

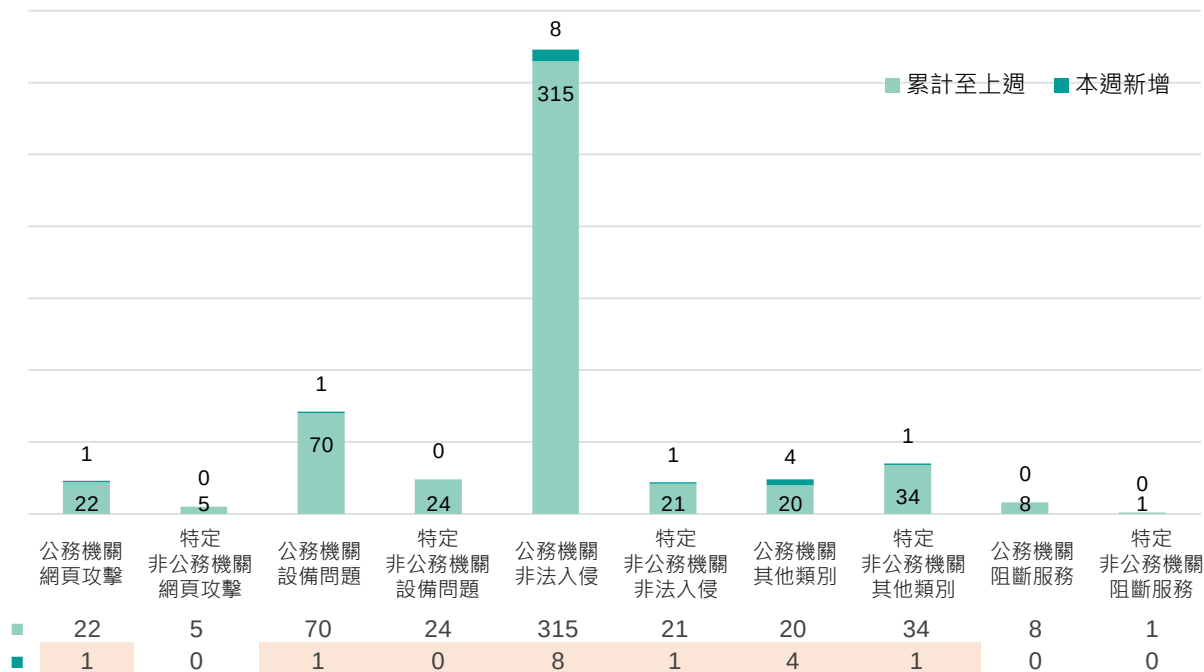


圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

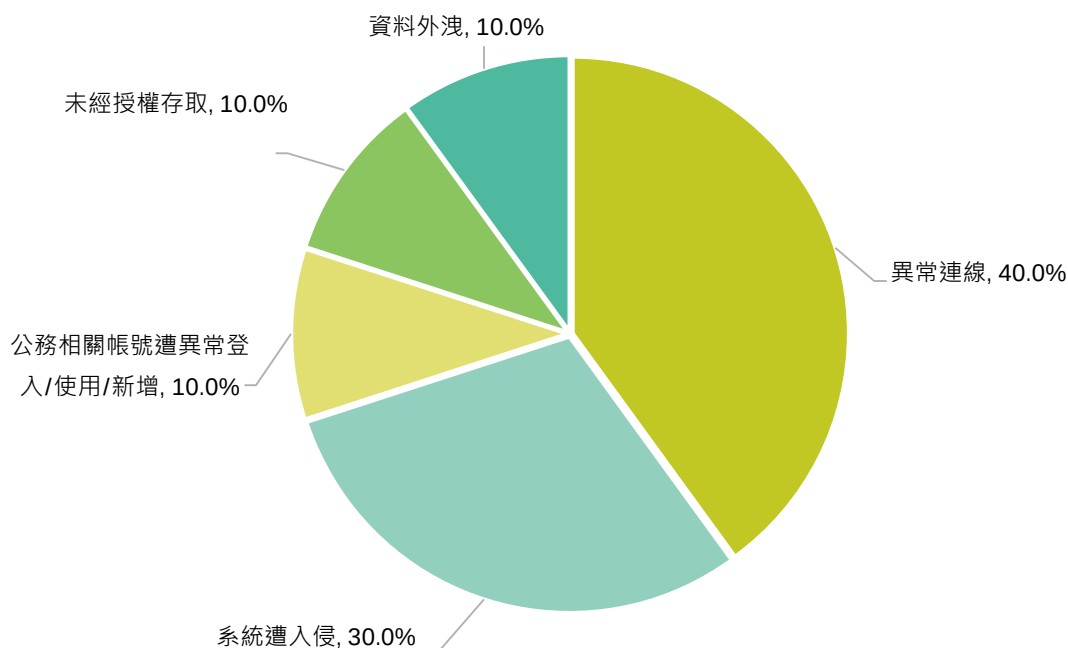


圖6 | 本週公務機關非法入侵事件類型占比

防護建議

除修補漏洞外，應：

以攻擊為出發評估潛在風險

- 攻擊者未經登入即可直接呼叫API取得資料
- 空白或異常請求未遭拒絕導致資料外洩

針對潛在風險執行相應改善

- 每次API請求均應執行身分鑑別，禁止未登入使用者直接存取資料
- 依帳號角色與業務權限檢核資料範圍，避免越權查詢非授權資訊
- 驗證必要參數、格式及內容完整性，拒絕空白或異常API請求
- 定期檢視測試及正式環境API設定，避免相同存取控制缺失同步存在

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，產業類別為其他電子業、電子零組件業、電腦及週邊設備業，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
貿聯控股	2026年08月24日	貿聯公司偵測到部分系統異常後，已立即啟動資安應變機制與隔離受影響之資訊系統措施，進行全面清查與復原作業，並同步委請外部資安專家協助復原與調查，後續將持續提升網路與資訊基礎架構之資安防護，以確保資料安全與營運韌性。
偉訓科技股份有限公司	2026年08月30日	偉訓公司偵測到部份資訊系統異常後，已立即啟動資安應變機制，並採取受影響資訊系統隔離及風險控管措施，且進行全面性盤點及持續監控，同時委請外部專業資安廠商協助進行系統復原、事件調查及相關強化作業。目前評估沒有個資、亦沒有機密或重要的文件資料外洩等情事發生，對本公司營運無重大影響。後續將持續依事件調查結果檢視並強化相關資訊系統及資安防護機制，並持續精進資安管理措施，確保資料安全及營運韌性。
富驊企業股份有限公司	2026年08月30日	富驊公司偵測到部份資訊系統異常後，已立即啟動資安應變機制，迅速採取受影響資訊系統隔離及風險控管措施，並進行全面性盤點及持續監控，同時委請外部專業資安廠商協助進行系統復原、事件調查及相關強化作業。

公司名稱	發布時間	事件說明
富驊企業股份有限公司 (續)		目前評估沒有個資、亦沒有機密或重要的文件資料外洩等情事發生，對本公司營運無重大影響。後續將持續依事件調查結果檢視並強化相關資訊系統及資安防護機制，並持續精進資安管理措施，確保資料安全及營運韌性。

■ 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

權威健康話術回升 翡翠團購與私訊導流升溫

詐騙類型趨勢

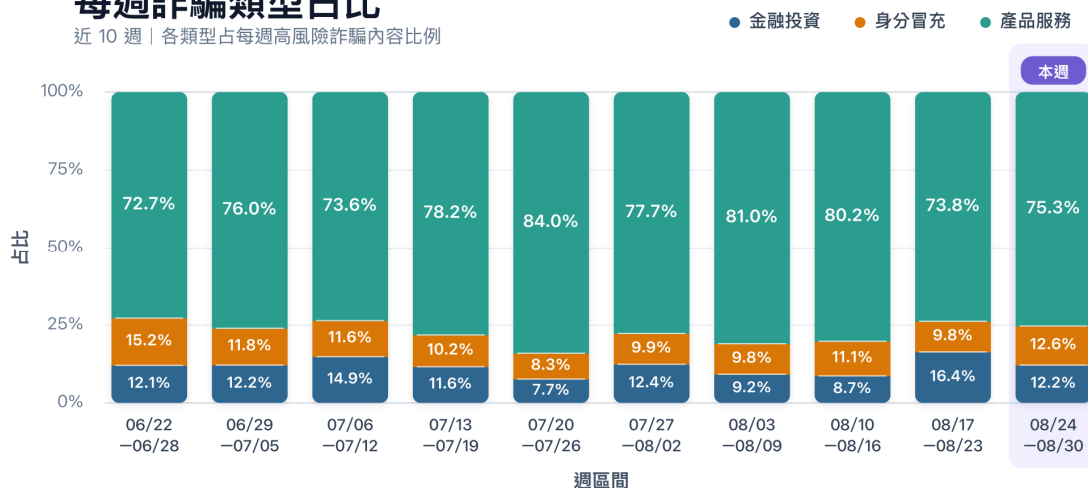
本週金融投資型占比明顯回落，並略低於身分冒充型。相關內容仍透過投資教學、熱門標的、免費觀察名單及博弈資訊吸引民眾，再以資金管理、進出場判斷及限時領取等說法，引導點擊連結或加入後續聯繫流程，詳見圖7。

身分冒充型占比回升。相關內容大量借用醫師推薦、臨床驗證、專業機構鑑定及講師經歷建立信任，並搭配具體改善數字、權威證書及成功案例，塑造專業人士或第三方機構背書的形象。

產品服務型占比回升，仍是本週主要高風險類型。內容涵蓋護眼與指甲保養產品、翡翠訂製、服飾團購、人工智慧行銷課程及交友招募等，常以免費體驗、大幅折扣、限量名額、真品保證及限時收單促使民眾行動，再導向私訊、社群或陌生連結。

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：2026/06/22—08/30

圖7 | 每週詐騙類型占比

關鍵字趨勢

「優惠」升至本週首位，詳見圖8，主要運用免費體驗、限量名額及具體改善數字推廣護眼產品。「配方」升至第 2 名，相關內容以天然草本、溫和不刺激及居家使用包裝指甲保養產品。「免費」則退居第 4 名，應用情境由商品促購轉向人工智慧行銷課程及限額報名。

「翡翠」升至本週第 3 名，相關內容以天然材質、產地說法、真品保證、工廠經營及口碑見證建立可信度。「團購」升至第 5 名，並與「直接」共同呈現大幅折扣、免運、限時收單、私訊詢價及加入社群等促購流程。

「直播」與「交友」新進本週 Top 10，分居第 6 名及第 7 名。前者以免費課程、限量席次及內容變現吸引報名；後者以單身交友、聊天陪伴及主動回覆吸引互動。「限量」與「健康」則分居第 9 名及第 10 名，持續透過稀缺感與專業健康形象強化商品吸引力。整體而言，本週話術由免費促購進一步轉向權威背書、社群團購及私密互動導流。

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 8/17-8/23 ● 本週 8/24-8/30

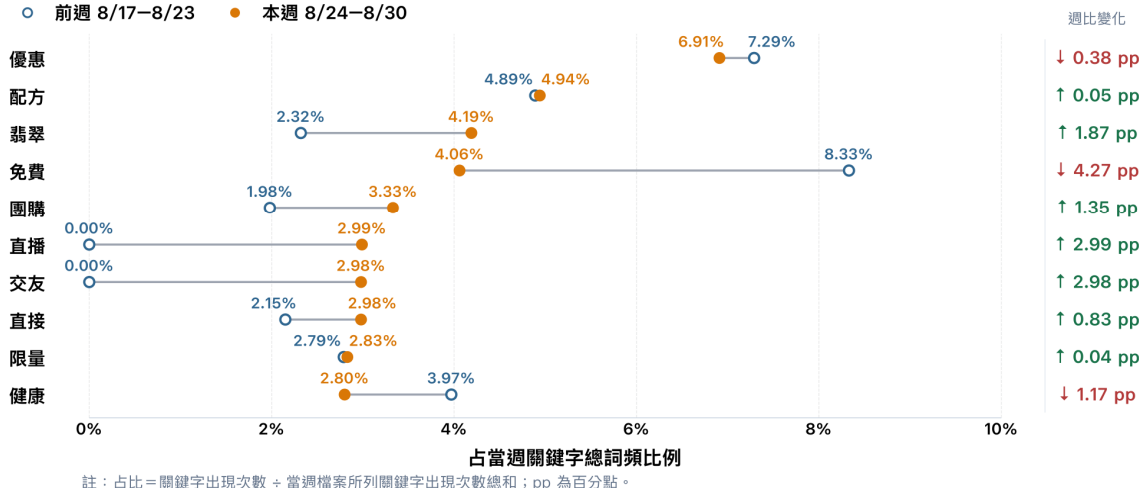


圖8 | 詐騙關鍵字占比週比變化

焦點文章

資安情資分享與威脅趨勢報告

從邊緣設備憑證外洩到 ERP 勒索的演變與防禦

根據 TWCERT/CC 上半年接獲情資統計，系統漏洞為最主要的資安情資類型，其次為勒索軟體攻擊，詳見圖9。由統計趨勢可觀察到，系統漏洞與勒索攻擊之間具有高度關聯性。近年攻擊者已逐漸將未即時修補的公開系統漏洞，作為取得初始存取權限的主要途徑，再進一步進行橫向移動、資料竊取及勒索軟體部署。

綜合近期情資與實際案例，許多企業組織遭遇勒索攻擊的根因可追溯至邊界設備的弱點或存取憑證遭到利用，例如 VPN、防火牆等設備存在未修補漏洞，或相關帳號憑證遭竊取，攻擊者掌握 VPN或防火牆憑證後，攻擊者得以取得初始存取權限並進一步進入內部網路。近期案例亦可觀察企業核心營運系統(ERP)遭列為攻擊目標，已成為各產業必須嚴加防範的關鍵資安風險。

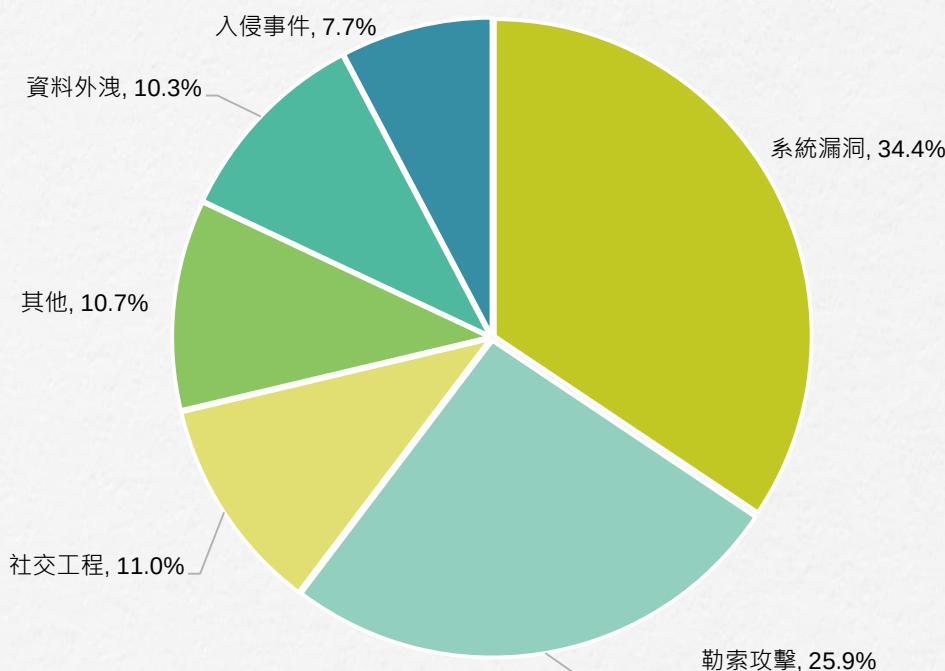


圖9 | TWCERT/CC 上半年接獲情資統計

焦點文章

AI 加速下的漏洞攻擊與自動化威脅

根據上半年接獲情資統計，系統漏洞依舊佔大宗，且漏洞被利用的速度顯著加快，生成式 AI 與自動化攻擊工具的普及為主要原因之一。以往漏洞公告至出現攻擊程式需數天甚至數週；如今攻擊者利用生成式 AI 輔助逆向工程，在漏洞細節公開後的數小時內即可生成攻擊腳本與自動化工具。

結合自動化掃描器與 AI 技術，攻擊者能對公開暴露的服務(如入口網站、VPN、邊緣設備)進行不間斷的探測，表示漏洞一旦揭露，即刻進入「全網自動搜捕」狀態。修補時間差因而攻擊者切入點，許多企業受限於內部變更審核流程或維運考量，無法及時完成修補，導致未即時修補的企業陷入高風險。

勒索攻擊趨勢由「無差別攻擊」轉向「供應鏈與關鍵系統癱瘓」

隨著企業備份機制日趨完善，傳統「僅加密檔案」的勒索效益顯著下降。攻擊者已轉向「機密資料竊取」，優先轉移財務報表、核心技術與客戶個資等高價值資料；即使企業還原系統，攻擊者仍會以公開機密、通報監管機關或誘發法律裁罰進行二次勒索。

在入侵手法上，近半年觀察顯示「利用公開網路邊緣設備」與「核心系統的未修補漏洞」已超越社交工程釣魚郵件，成為勒索軟體即服務最主要管道，大幅縮短從滲透到勒索的時程。

其中，ERP 系統因整合財務、供應鏈與員工等核心營運資料，且部分系統或模組因業務需求直接暴露於網際網路，且通常涉及較多權限，因此可能成為勒索攻擊的目標。攻擊者通常利用未修補的遠端程式碼執行漏洞，在未經正常身分驗證的情況下取得伺服器控制權；在加密系統前，亦可能先竊取財務報表及客戶個資，作為後續勒索的籌碼。一旦 ERP 系統遭到加密或癱瘓，企業營運將瞬間陷入停擺，並增加企業處理勒索事件的壓力。

新型勒索軟體組織的威脅演變與特徵

隨著舊有知名勒索集團陸續遭國際執法機構打擊或內部分裂，上半年情資顯示大量新型、高度碎片化且彈性更高的勒索軟體組織迅速崛起。這類組織不再耗時進行第一階段的初次滲透，而是轉向暗網大量購買外洩憑證或已知/未知漏洞的存取權，大幅提升攻擊效率。

焦點文章

因應現代企業普遍採用 VMware ESXi 虛擬化平台與 Linux 環境，新型勒索軟體具備強大的跨平台編譯能力。攻擊程式能在數秒內強制關閉資料庫服務與虛擬機進程，直接針對底層虛擬機磁碟檔(.vmdk)與 Linux 資料庫發動高強度加密。這種「直擊營運核心」的攻擊，壓縮了企業的應變與復原時間，使得營運陷入停擺的風險急劇上升。

結語

綜觀 TWCERT/CC 上半年的接獲資安情資與趨勢分析，企業正面臨一場攻防防線與反應速度極度不對稱的嚴峻考驗。攻擊者已整合「AI加速漏洞攻擊」、「暗網購買外洩憑證」與「新型跨平台勒索軟體」，建構出一條由外圍邊界直擊內網核心的攻擊鏈。面對修補時間差被大幅壓縮的現狀，企業防禦策略應提早作好準備：

1. 定期檢視對外服務與邊界設備漏洞：盤點 VPN 閘道器、防火牆及遠端桌面(RDP)等對外服務。定期檢視相關設備及系統是否存在已知漏洞，並依風險及時完成修補與更新，降低對外服務遭利用的風險。
2. 落實離線與不可篡改備份機制：落實 3-2-1 備份原則，將關鍵資料庫之備份檔儲存於實體隔離或獨立網段的安全空間，並啟用「不可篡改」防護特性，確保遭勒索攻擊時仍具備營運復原。
3. 實施網段微隔離與權限最小化：依業務功能進行網路區域劃分，嚴格限制網段間的不必要連線；針對伺服器、NAS 及 VDI 等關鍵資源實施嚴格存取控管，阻斷攻擊者於內網橫向移動與擴大破壞範圍。
4. 啟用多因子驗證(MFA)與帳號治理：針對 VPN、企業郵件及高權限帳號啟用 MFA，並定期清查無效、預設及長期停用之帳號。同時應注意 Session Token 遭竊取或釣魚攻擊繞過 MFA 的風險，適時檢視身分驗證機制。
5. 強化異常活動監控與事件應變機制：建立邊界設備、AD 主機、伺服器與端點之日誌集中蒐集與監控，重點監控異常登入、權限變更、大容量資料傳輸及日誌清除行為。發現可疑活動時，應依既有事件應變程序進行確認及處置，必要時隔離受影響設備或限制相關連線，以降低事件影響範圍。

關鍵字：勒索攻擊、AI自動化漏洞威脅、邊緣設備憑證外洩

刊 名 資安週報第 60 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