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

資安週報

Cyber Security Weekly Newsletter

2026.08.20
058

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

主要風險項目多呈下降 未部署WAF改善幅度較明顯

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2,864項。其中，「元件高風險漏洞」以931項居首，「過時或弱加密協定」831項次之，「TLS憑證不受信任」589項位居第三。前三項合計2,351項，占前10大風險項目總數約82.1%，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2,919項，整體風險數量僅減少55項(約1.9%)；前三項占比則由約81.8%微增至約82.1%，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940項微降至931項，降幅約1.0%。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Apache HTTP Server目前最新穩定修補版本。Apache官方確認CVE-2024-38475影響2.4.59以前版本，並自2.4.60修補；目前官方亦建議採用最新穩定版本，而非停留於早期修補版本。本期檢測出Drupal所使用之PEAR Archive_Tar函式庫相關弱點(CVE-2020-36193)，可能導致目錄遍歷風險。Drupal官方確認該弱點涉及其使用之PEAR Archive_Tar第三方函式庫。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Drupal 11.4.x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840項微降至831項，降幅約1.1%；「TLS憑證不受信任」由607項降至589項，降幅約3.0%。另在網站防護設定方面，「CSP設定不當」由251項微降至247項，降幅約1.6%；「未部署WAF」由144項降至125項，降幅約13.2%。整體而言，本期主要風險項目多呈下降趨勢，而「未部署WAF」改善幅度較為明顯，前10大風險總量較上期小幅收斂。

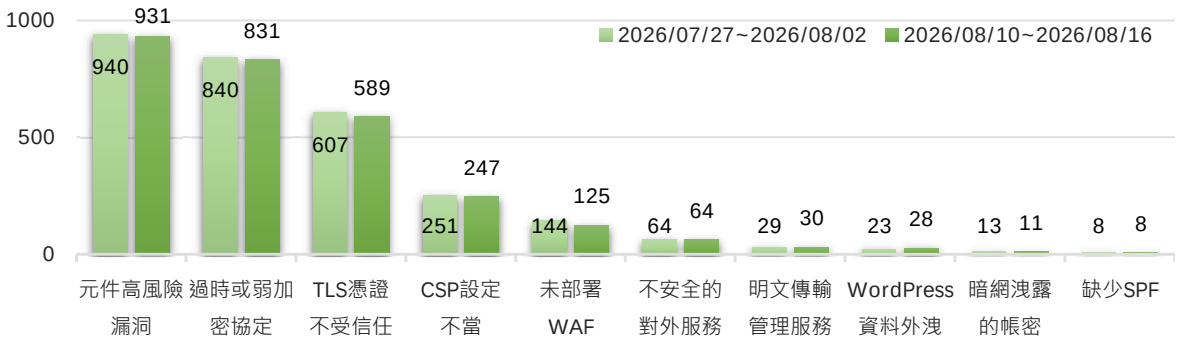

圖1 | EASM檢測結果統計(前10大風險)

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
➢ 優先修補對外服務之高風險元件漏洞，並依原廠公告更新至已修補版本；如無法立即升級，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 ➢ 依據IETF RFC 10015建議在TLS 1.2中停用靜態RSA(如TLS_RSA_WITH_*)、有限域 DH(如TLS_DH_*)及DHE(如TLS_DHE_*)等密碼套件，並避免使用靜態ECDH(如 TLS_ECDH_*)之密碼套件，優先採用ECDHE等具前向保密性之安全金鑰交換機制 ➢ 強化TLS憑證管理，定期確認憑證有效性、信任鏈及到期日，並建立憑證到期監控與自動續期機制 ➢ 檢視網站CSP與WAF等安全防護設定，依實際業務需求調整安全政策，降低網站遭受跨網站腳本、惡意請求或其他Web攻擊之風險	➢ 建立並定期更新對外資產、IP、網域、系統元件及憑證清冊，掌握資產版本與用途 ➢ 建立高風險漏洞修補與追蹤機制，依漏洞嚴重程度訂定修補時限，並於完成修補後進行複測確認 ➢ 定期盤點系統使用之軟體及第三方元件版本，持續關注原廠安全公告及CVE資訊，避免使用已停止支援或存在已知漏洞之版本 ➢ 將漏洞修補、憑證更新、安全設定及複測要求納入委外維運管理機制，明確訂定處理時限與權責，確保改善措施落實

■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Cisco高風險漏洞應盡速修補

- 微軟釋出115年8月份安全性更新，共修補包含Microsoft Teams、Azure SQL Database及Microsoft Planetary Computer Pro等共419個漏洞[1]，其中包含61個高風險漏洞，且CVE-2026-68820已遭駭客利用。

- Cisco Integrated Management Controller(IMC)存在高風險漏洞(CVE-2026-20200)[2]，類型為存在不當處理參數分隔符號(Improper Neutralization of Parameter/Argument Delimiters)，已取得低權限之遠端攻擊者，可利用此漏洞以root權限執行任意指令。

- Cisco IOS XE Software存在2項高風險安全漏洞(CVE-2026-20267與CVE-2026-20272)[3]，類型分別為不當存取控制(Improper Access Control)與注入(Injection)。未經身分鑑別之遠端攻擊者可利用該等漏洞，造成系統機密性、完整性及可用性受影響。

- Cisco Catalyst SD-WAN存在4項高風險安全漏洞(CVE-2026-20303、CVE-2026-20304、CVE-2026-20310及CVE-2026-20312)[4]，類型分別為不當輸入驗證(Improper Input Validation)、不當存取控制(Improper Access Control)、連結追蹤(Link Following)及以明文方式儲存敏感資訊(Cleartext Storage of Sensitive Information)。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、完整性及可用性受影響。

1. https://msrc.microsoft.com/update-guide/releaseNote/2026-Aug
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-arg-inject-upSHdMfU
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
4. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K

■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

實兵演練揭露檔案存取控管失效 致系統敏感檔案遭未授權存取風險

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8/14止已累計269筆攻擊紀錄，本週新增弱點數量共4筆，分別為「無效的存取控管」2筆、「不安全的組態設定」1筆及「驗證機制失效」1筆，詳見圖2。

本週演練發現，衝擊性較高之弱點為「無效的存取控管」。攻擊者於系統操作過程中，透過Burp Suite工具檢視系統功能請求內容，發現存在「api/download」檔案路徑。攻擊者發現於封包內存在參數「url」，嘗試修改「url」參數內容為「../../etc/shadow」進行測試，發現系統未針對檔案存取路徑進行驗證與存取控管，導致可透過竄改檔案路徑，存取非原預期範圍之系統檔案，並取得作業系統敏感檔案內容，造成系統資訊洩漏之風險。

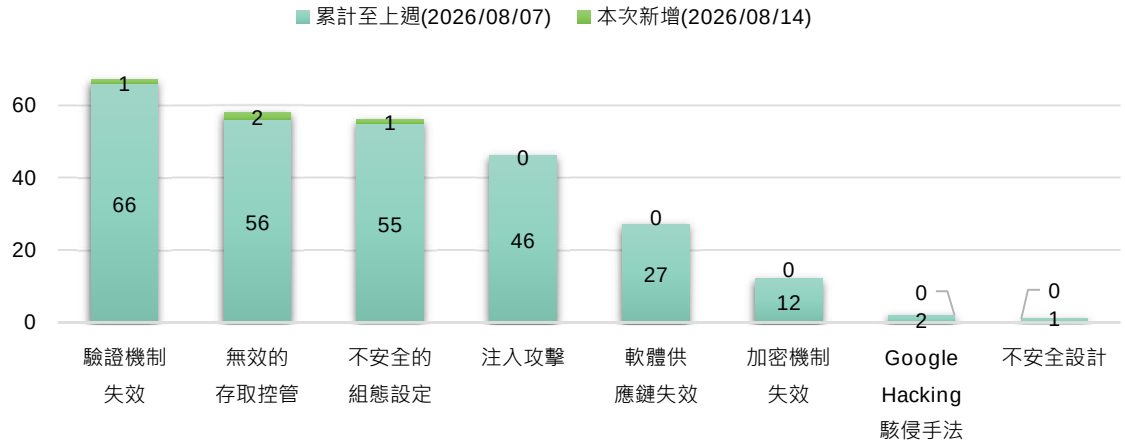

圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應全面檢視系統各項檔案下載、查詢及資料存取功能權限，確認僅能存取所需之檔案與資料
- 應建立系統功能與 API權限之定期檢視機制，針對新增、異動或變更之功能進行權限控管複查，確認使用者存取權限符合實際需求，避免因功能調整或權限設定異動造成存取控管失效
- 檔案下載功能應於伺服器端實施身分驗證與存取權限控管，避免直接使用使用者輸入之參數指定檔案路徑，並限制應用程式可存取之目錄範圍。另應對檔案路徑進行適當之驗證，以防範目錄遍歷(Path Traversal)等攻擊，降低未經授權存取系統敏感檔案之風險

■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

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14.2%，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12.1%，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。

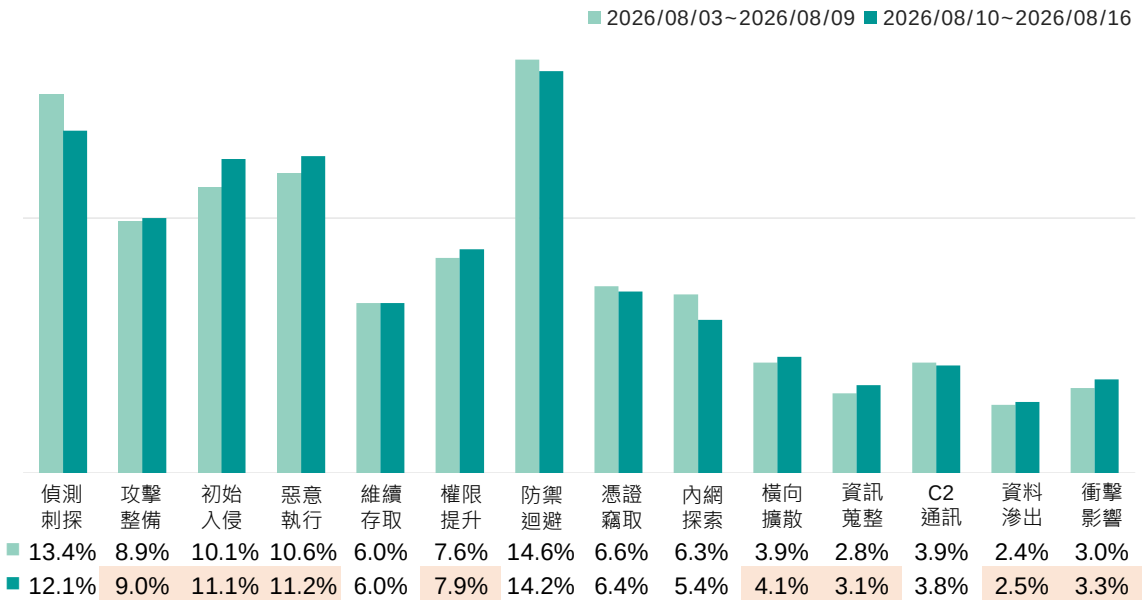

圖3 | 資安聯防監控攻擊階段統計

防護建議

建議機關採取下列防護措施

防禦迴避(Defense Evasion)

- 導入並強化端點偵測與防護機制(EDR)
- 加強指令與系統操作紀錄之留存及稽核
- 限制高風險或可被濫用之合法系統工具
- 落實特權帳號與權限控管，降低攻擊者規避偵測的風險

偵測刺探(Reconnaissance)

- 加強監控異常掃描、IP區段探測及帳號探測行為
- 定期盤點對外暴露之系統、服務及開放埠，降低攻擊面
- 持續檢視公開或外洩之帳號、憑證相關資訊
- 結合威脅情資識別可疑來源，及早阻擋潛在攻擊活動

■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75.59%、「遠端控制」服務攻擊占比19.53%，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77.35%。「遠端控制」服務亦有19.42% 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Cisco Secure ASA & FTD軟體存在授權缺失漏洞之CVE-2025-20362，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。

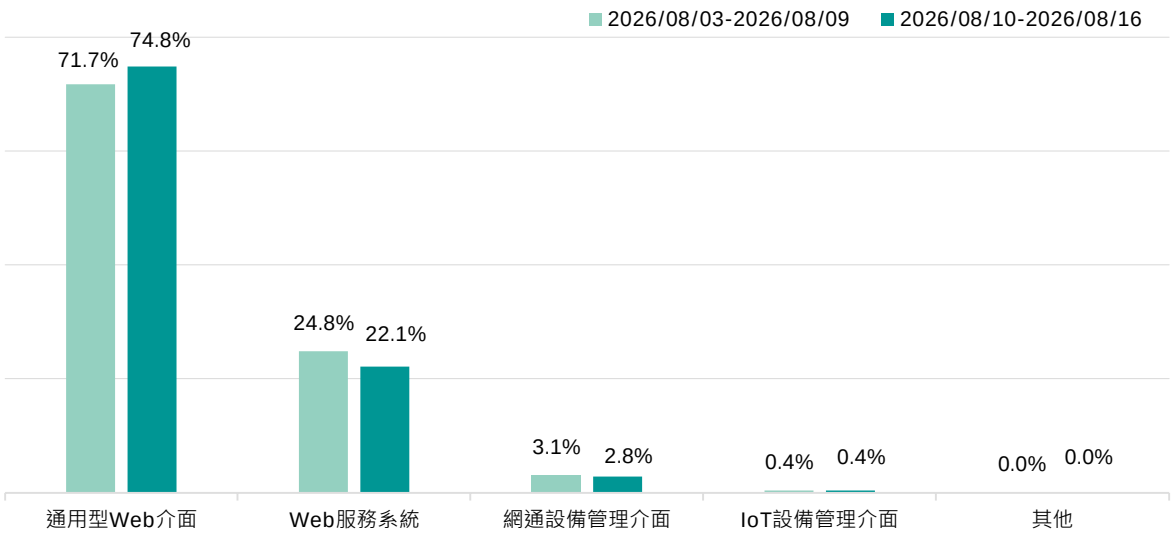

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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指令注入漏洞、身分驗證繞過漏洞、越界讀取漏洞及程式碼注入漏洞，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、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	↑1	CVE-2026-42271[1]	LiteLLM	8.8	✓
■	2	↑1	CVE-2026-41940[2]	cPanel & WHM	9.8	✓
■	3	↑1	CVE-2026-3055[3]	NetScaler ADC & Gateway	9.8	✓
■	4	↑new	CVE-2026-1281[4]	Ivanti Endpoint Manager Mobile	9.8	✓
■	5	↑new	CVE-2026-1340[5]	Ivanti Endpoint Manager Mobile	9.8	✓

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

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-2026-3055
4. https://nvd.nist.gov/vuln/detail/CVE-2026-1281
5. https://nvd.nist.gov/vuln/detail/CVE-2026-1340

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

前端可取得之憑證 應避免具備不必要的後端存取能力

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占多數，詳見圖6。本週發現機關網站於使用者尚未登入前，即可於前端載入之JavaScript取得JWT，且該憑證可直接用於另一後端服務呼叫API並取得系統資料。

由於前端程式內容可由使用者檢視，具資料存取能力之憑證若於登入前即可取得，可能使原有身分驗證及存取控制機制失去預期效果。建議機關清查登入前載入之 JavaScript、前端設定檔及伺服器回傳內容，確認是否含有 JWT、API Key 或其他可存取後端服務之憑證，並釐清其用途與權限範圍。若業務上確有前端使用憑證之需求，例如提供匿名查詢功能，應限制可使用之功能及資料範圍，並由後端僅回傳必要資料；已暴露之憑證則應停用或更換，並以未登入狀態重新測試，確認無法再利用原憑證存取受影響 API。

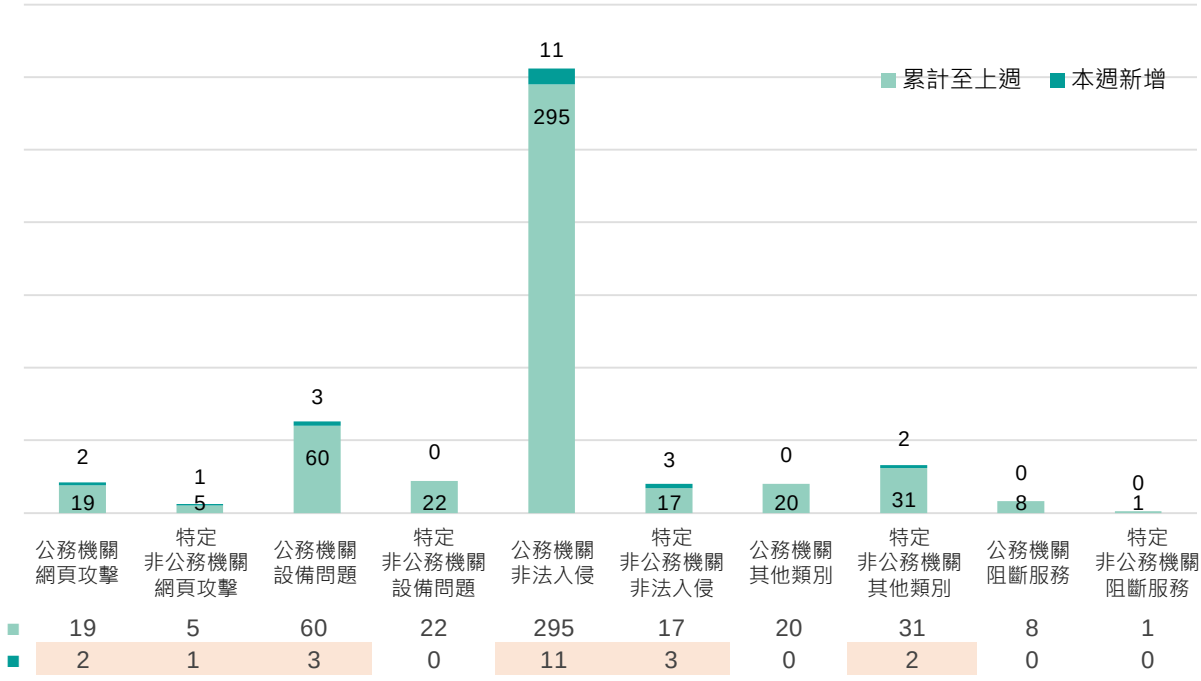

圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

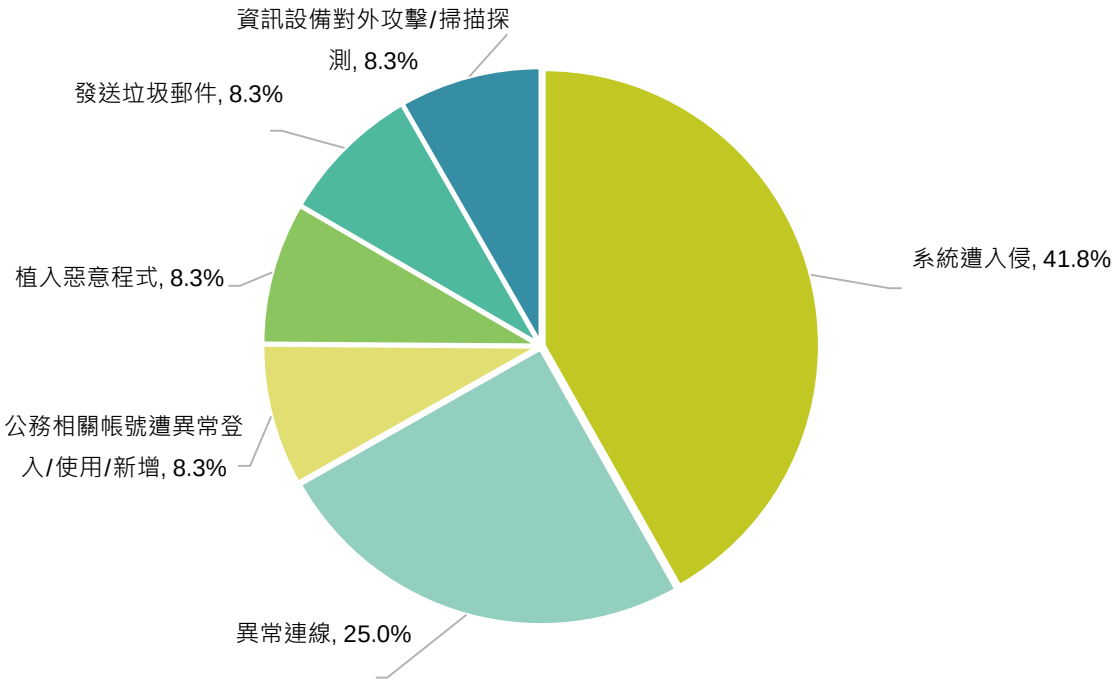

圖6 | 本週公務機關非法入侵事件類型占比

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
➢ 未登入即可取得具存取能力JWT，可能遭濫用繞過身分驗證取得系統資料 ➢ 前端暴露API憑證與權限資訊，恐造成未授權查詢、資料外洩及後續入侵	➢ 清查前端JavaScript與設定檔，移除JWT、API Key等敏感存取憑證 ➢ 限制匿名憑證可存取功能與資料範圍，後端僅回傳業務必要資訊 ➢ 強化後端API身分驗證與授權檢核，避免僅依憑證有效性決定存取 ➢ 立即停用或更換已暴露憑證，並以未登入狀態重新驗證存取控制

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，產業類別皆為生技醫療業，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
久裕企業股份有限公司	2026年08月10日	久裕公司部分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。初步評估對公司營運無重大影響，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。
	2026年08月11日	久裕公司於8月11遭受駭客針對復原系統再次攻擊，經外部資安公司協助排查，遭加密之資料恐有外洩疑慮，核心系統及資料庫並未受影響，目前已配合外部資安公司採取因應措施、啟動資安相關防禦機制與應變作業並通報相關機關，後續將繼續尋找資安專家協助，改善及提升資安機制。
正瀚生技股份有限公司	2026年08月11日	正瀚公司部分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。初步評估對公司營運無重大影響，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。

■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

身分包裝升溫 免費博弈與保健功效話術擴散

本週金融投資型占比減少 0.5 個百分點。相關內容持續以低價潛力股、數倍報酬及免費股票代碼吸引民眾，並透過投資課程、選股工具與市場趨勢分析包裝專業性，再引導點擊連結或私訊領取資料。占比雖略為下降，免費資訊、教學內容與私訊導流仍是主要接觸方式，詳見圖7。

身分冒充型占比增加 1.3 個百分點，為三類中唯一上升的類型。相關內容大量運用醫療機構、醫師、專科權威及命理老師等身分建立信任，包括宣稱獲醫師推薦、臨床驗證、醫療機構主管背書，以及以專家身分提供感情或命盤諮詢。此類權威身分包裝帶動身分冒充型占比回升。

產品服務型占比減少 0.8 個百分點，仍占整體八成。高風險商品與服務涵蓋中古車貸款、指甲修護產品、草本保健品、翡翠飾品、隨行熱水設備、防水噴劑及生髮產品等。常見手法包括境外技術、天然配方、精確療效數字、低價優惠、正品保證及限量促銷，再透過表單、私訊或陌生連結完成交易，產品服務型持續是本週最主要的高風險類型。

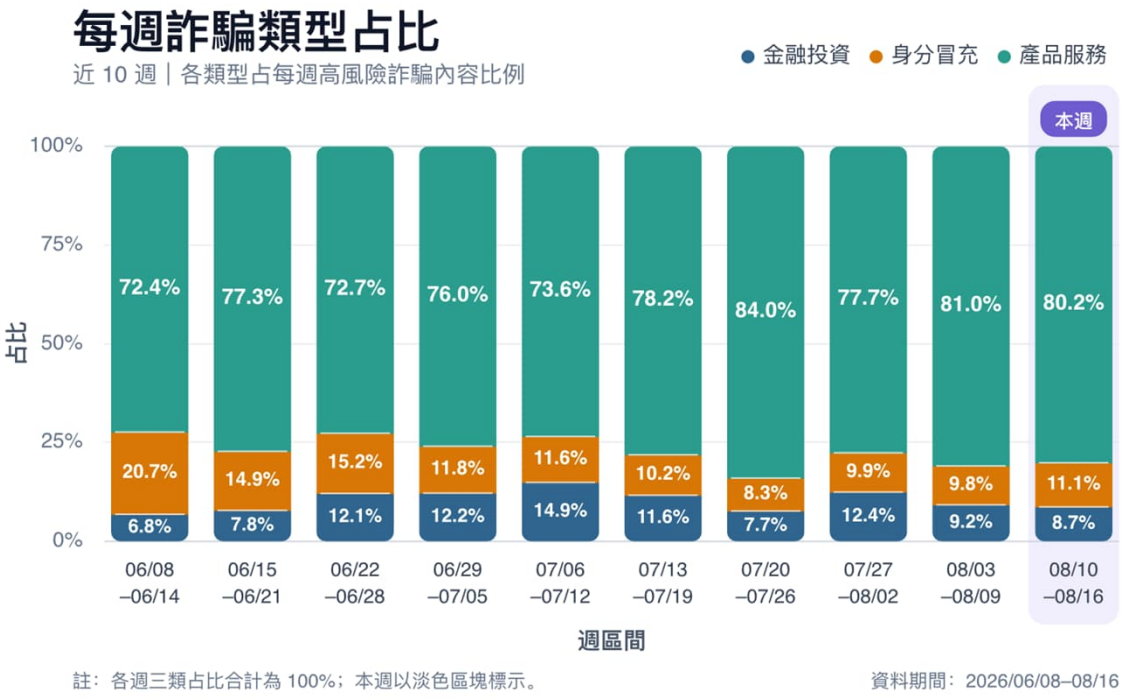

圖7 | 每週詐騙類型占比

「優惠」占比增加 2.09 個百分點，持續位居本週首位。相關話術由投資課程轉向中古車與貸款方案，以低利率、免頭款、全額貸款及贈品降低交易門檻，再透過試算表單與通訊帳號承接聯繫，詳見圖8。

「免費」占比增加 1.99 個百分點，升至本週第二名。相關內容以免費博弈分析公式及操作資料吸引民眾，搭配大量詢問人數與私訊領取等說法，導入後續一對一聯繫。

保健醫療話術持續受到運用。「配方」增加 1.48 個百分點；「健康」減少 2.00個百分點，仍居本週第四名；「日常」增加 3.29 個百分點，新進第五名。相關廣告以天然成分、臨床驗證、醫師認可及短期見效包裝產品，並將呼吸道調理與體質改善塑造成日常養生習慣。

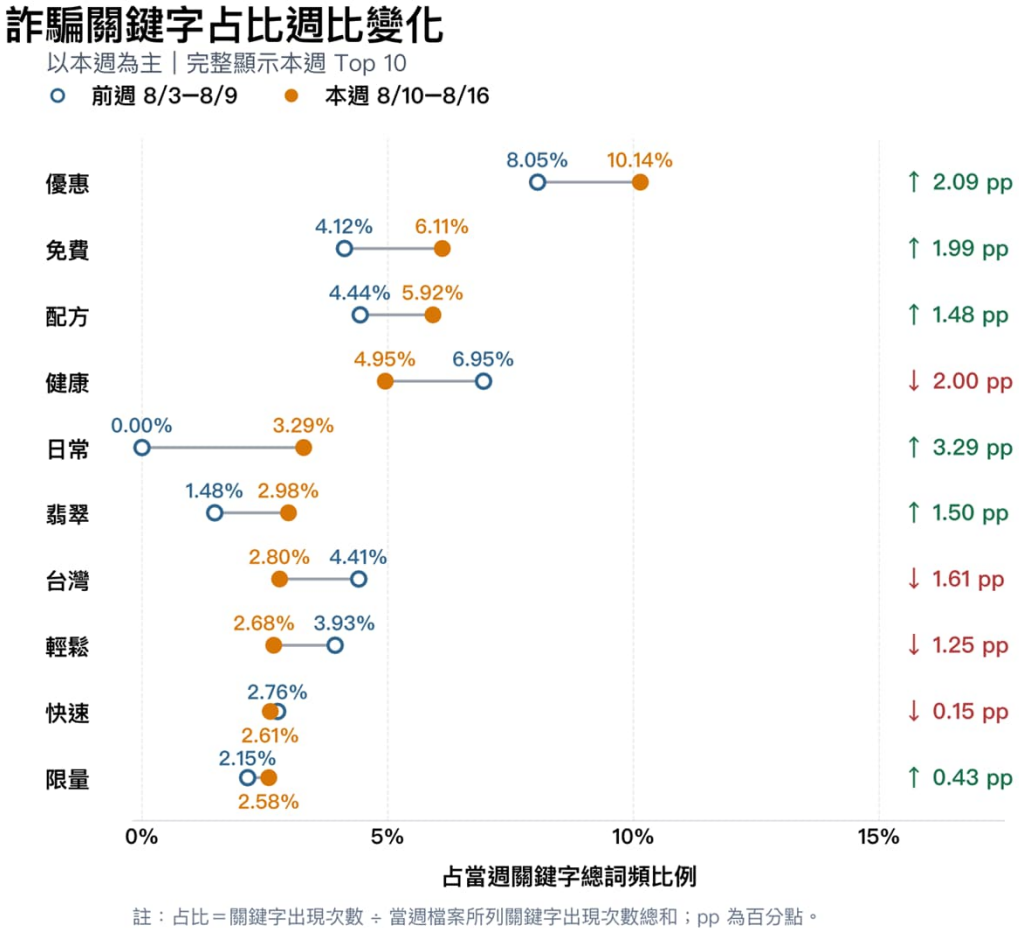

圖8 | 詐騙關鍵字占比週比變化

「翡翠」占比增加 1.50 個百分點，相關內容以低價訂製、天然產地、正品保證及工廠經營年資建立可信度。「台灣」與「輕鬆」分別減少 1.61 及 1.25 個百分點，主要反映隨行熱水設備運用台灣熱銷、快速加熱及便攜操作包裝便利性。

「快速」減少 0.15 個百分點，仍維持前十名，著重快速止漏及耐用功效；「限量」增加 0.43 個百分點，以限定組數、售完為止及短期見效製造急迫感。整體而言，本週主要話術集中於促銷優惠、免費導流、保健功效、日常養生與限量稀缺性。

焦點文章

115年上半年CISA KEV漏洞利用趨勢分析

近年資安漏洞增長速度已達到前所未有的規模[1]，面對龐大且分散的漏洞資訊，企業常陷入「漏洞修補疲勞」，難以在有限資源下判斷哪些漏洞應優先處置。為了應對此挑戰，美國國土安全部(DHS)轄下的網路安全暨基礎設施安全局(CISA)[2]持續維護「已被成功惡意利用漏洞清單」(Known Exploited Vulnerability Catalog，簡稱KEV)[3]。CISA KEV核心價值在於其實戰性，讓防禦單位更能聚焦「駭客正在利用」的漏洞。根據CISA規範[4]，漏洞被納入KEV須符合三項條件分別為：(1)該漏洞必須具備正式的CVE編號、(2)必須有可靠的證據證明該漏洞已在實際攻擊中被惡意利用、(3)必須具備明確且可執行的緩解措施或修補建議。以下分析今年上半年CISA KEV漏洞利用趨勢。

1.1 漏洞影響系統類型與廠商分布

在漏洞所屬廠商分布上，微軟(Microsoft)、思科(Cisco)及蘋果(Apple)為115年上半年KEV中占比最高的前三大廠商，相關廠商漏洞數量統計詳見圖9。

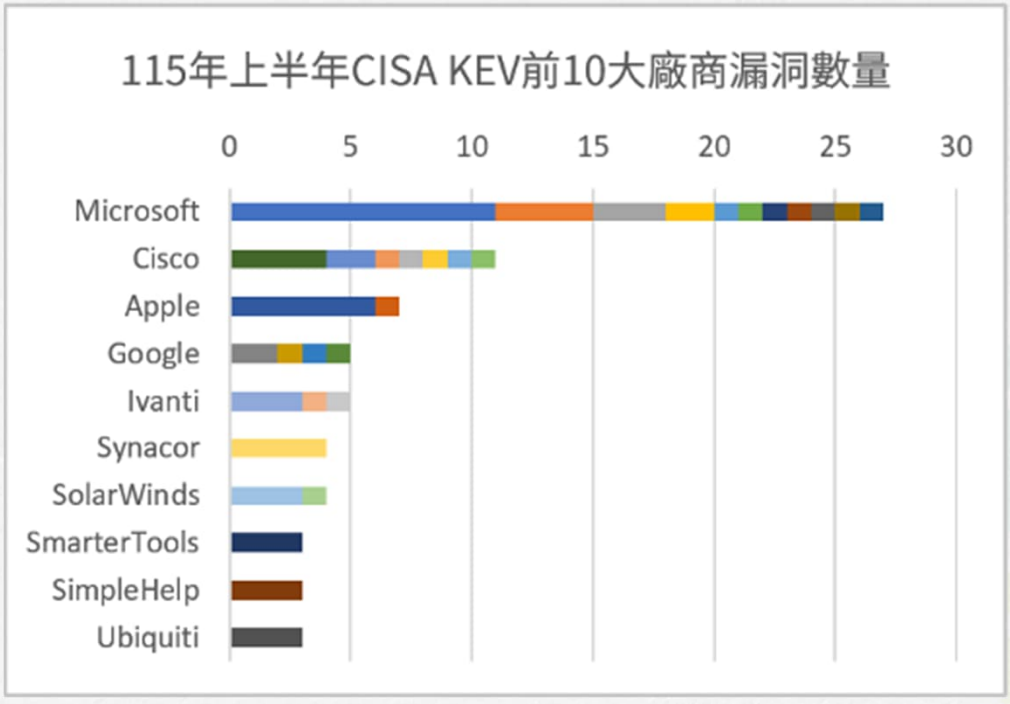

圖9 | 115年上半年CISA KEV前10大廠商漏洞數量

焦點文章

依據數量統計，說明如下：

1. 微軟產品漏洞多集中在Windows作業系統與SharePoint等協作平臺，由於其極高的市場佔有率使其常成為駭客目標。
2. 思科產品多為設備管理相關的網通設備，反映網路基礎設備在邊界防禦中的脆弱性。
3. 蘋果產品的漏洞增加則與行動設備與macOS作業系統在企業環境中的普及密切相關。

分析駭客常見攻擊的目標，可分為作業系統類、設備管理類及電子郵件類。此外，值得關注115年出現的新興攻擊目標趨勢為駭客針對AI生態系工具、端點資安管理及遠端管理工具的攻擊，相關說明如下。

1. 作業系統類(如Microsoft Windows、Apple iOS及Linux)是駭客主要攻擊目標，因此類系統為所有應用程式的基石，一旦失守即代表整台設備被完全控制。
2. 設備管理類(如Cisco Catalyst SD-WAN Manager、Ivanti EPMM及VMware vCenter Server)的漏洞頻率顯著上升，這顯示駭客正試圖透過基礎設施漏洞獲取更廣泛的滲透權限。
3. 電子郵件系統類(如Zimbra Collaboration Suite、SmarterMail及Roundcube Webmail)常涉及機敏資訊且暴露於網際網路上，亦成為上半年的攻擊熱點。
4. AI生態系工具類，隨著企業加速導入人工智慧模型，AI工具漏洞開始被收錄進KEV，代表駭客已具備針對AI供應鏈進行攻擊的能力。
5. 端點資安管理類，資安廠商推出的端點資安管理產品其作為組織邊界防禦的特性，一旦存在漏洞，反而成為駭客繞過所有防護進入內網的快速途徑。
6. 遠端管理工具類，駭客惡意利用漏洞以接管受控系統與設備的主導權，往往會直接利用工具內建合法管理功能對設備進行操控。這類攻擊手法不僅能實現對設備的全面接管，更因其利用既有功能進行作業，大幅增加企業在偵測惡意行為的困難。

1.2 攻擊類型與漏洞根因分析

分析漏洞手法發現，在眾多CWE弱點類別[5]中，前12大CWE涵蓋過半數CVE漏洞編號，顯示駭客的攻擊手法集中於特定的技術弱點，可歸類於5項弱點類別如下。

焦點文章

1. 程式碼執行類漏洞，包括「程式碼注入」與「作業系統指令注入」，這類漏洞導致駭客可遠端執行任意程式碼，達到遠端接管受駭系統。此外，「不安全的反序列化」也頻繁出現，這反映了應用程式在處理外部傳入資料時的結構性缺陷。
2. 存取控制類漏洞，驗證機制缺陷是另一大宗，包含「不當身分驗證」與「關鍵功能缺乏身分驗證」的氾濫，讓駭客能輕易繞過登入程序，直接存取受保護的資源或執行高權限操作。
3. 網頁安全類漏洞，「路徑遍歷」與「伺服器端請求偽造」常被組合使用，用以獲取系統內部敏感檔案或作為內網滲透的跳板。此外，傳統威脅如「跨網站指令碼」與「SQL資料隱碼」雖已存在多年，但仍榜上有名，顯示許多應用系統在輸入過濾上仍有疏漏。
4. 記憶體安全類漏洞，「記憶體釋放後使用」與「記憶體緩衝區限制不當」在低階語言開發的系統中依舊猖獗，這類漏洞往往導致系統崩潰或遠端程式碼執行。
5. 供應鏈攻擊類漏洞，「內嵌惡意程式碼」標誌著供應鏈攻擊的常態化，駭客在軟體開發階段即植入後門，增加了檢測的複雜度，這反映出程式開發過程中的安全驗證不足，是導致系統被攻破的根本原因。

1.3 攻擊路徑與條件分析 (CVSS Vector 統計)

分析漏洞對應的通用漏洞評分系統(Common Vulnerability Scoring System, CVSS)[6]，分析發現駭客的攻擊目的呈現「低門檻與高效益」特徵，4個分析面向說明如下，相關漏洞CVSS分析請詳見圖10。

漏洞分析部分，說明如下：

1. 攻擊向量(Attack Vector)方面，80.1%漏洞可透過網路惡意利用，代表駭客無需實體接觸設備，甚至不需要進入組織的區域網路，即可從世界任何角落發動攻擊，這增加了防護挑戰。
2. 所需權限(Privileges Required)方面，71.9%漏洞利用不需要任何權限條件，代表駭客可於不具備任何合法帳號情況下，對系統進行有效攻擊，這類未經授權的攻擊特性使駭客能輕易達成其目的。
3. 攻擊複雜度(Attack Complexity)方面，93.2%漏洞利用方式並不複雜，駭客不需特定前提條件即可成功惡意利用漏洞，大幅降低攻擊技術要求，使得自動化攻擊工具能被大規模運用。

焦點文章

4. 使用者互動(User Interaction)方面，77.4%漏洞不須與使用者互動即可觸發。這打破了「不點擊不明連結就安全」的迷思，駭客可單方面透過惡意手法觸發漏洞，受害者在毫無察覺的情況下即可能遭到入侵。

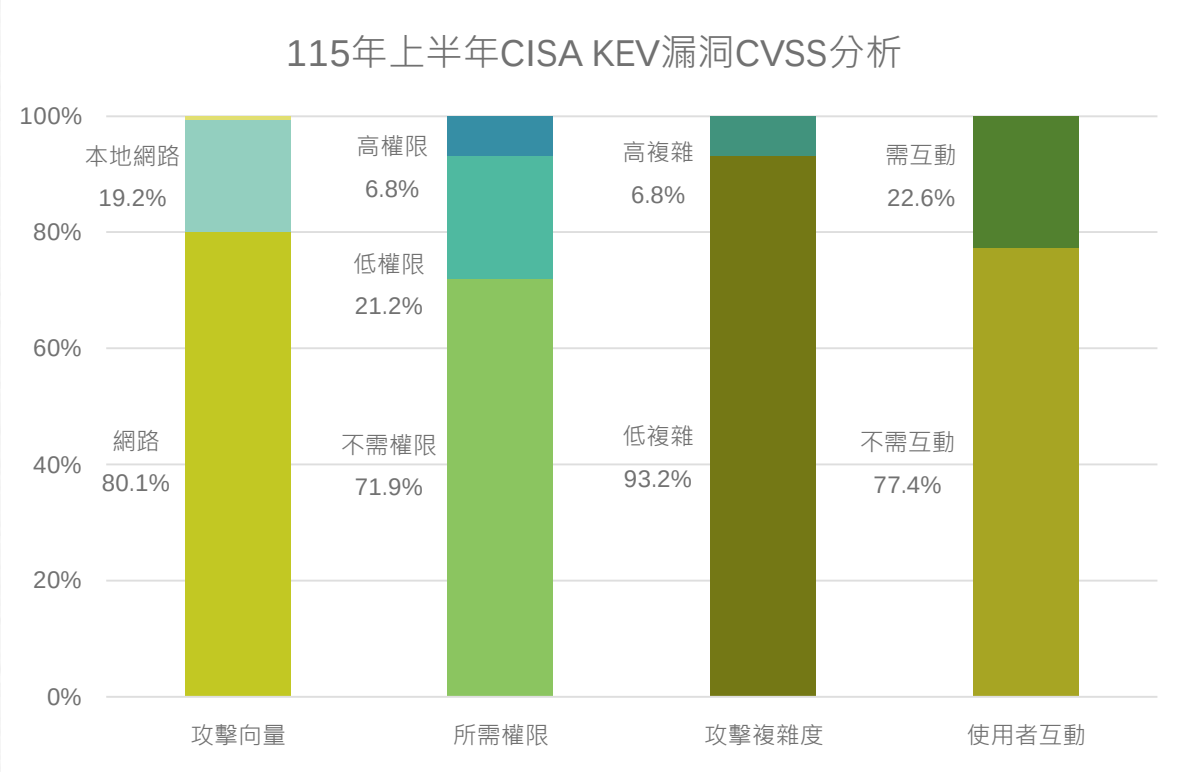

圖10 | 115年上半年CISA KEV 漏洞CVSS分析

綜合115年上半年CISA KEV漏洞之CVSS攻擊條件可見，駭客實際利用漏洞多集中在可經由網路遠端發動、無須預先取得帳號權限、利用步驟簡單，以及不需使用者互動的類型。換言之，企業對外提供服務的攻擊面(如網站、虛擬私人網路服務、防火牆、郵件系統)，以及民眾使用之連網設備(如無線路由器、網路儲存伺服器或網路監視器)，若存在已列入CISA KEV便可能成為駭客自動化掃描與入侵的目標。這反映CISA KEV所收錄的漏洞並非僅具理論風險，而是已確認遭駭客實際利用，其中多數又具有低門檻、易於重複利用與大規模擴散的特性。因此，這類漏洞一旦存在於對外連線的系統或設備中，可能在短時間內被發現並遭利用。

焦點文章

1.4 防護建議

針對115年上半年CISA KEV漏洞利用趨勢分析，資安院提供相關防護建議供參。

1. 企業應從被動漏洞修補轉向主動防禦。建議將CISA KEV整合進漏洞管理流程。不再僅依賴CVSS分數，而應將KEV中收錄的CVE視為最高優先級，因為這些漏洞已經被實際惡意利用，其威脅程度遠高於僅具備理論風險的高分漏洞。
2. 建議落實外部攻擊面管理(External Attack Surface Management, EASM)，企業須建立完善的資產盤點機制，持續確認組織是否有受KEV漏洞影響的連網設備。包括定期掃描對外暴露的IP、服務及設備，並與KEV進行比對。當確認內部存在漏洞影響設備時，可參照相關官方安全性更新建議，評估執行更新或其他緩解措施。
3. 企業應將資安防禦延伸至持續性監控。建議將資訊設備納入資安監控範圍，透過日誌關聯分析以識別網路異常行為，並捕捉可能的漏洞掃描或初期的入侵跡象，以在威脅發生前將風險降至最低。
4. 資安院也持續將KEV納入漏洞示警與資安風險管理流程[7]，檢視我國政府領域是否受相關漏洞影響，並優先告警政府機關處置受漏洞影響設備，以強化政府領域資安韌性。同時透過國家資安資訊分享與分析中心[8]，將漏洞研析情資分享予各領域，達到聯合防禦之綜效，提升國家資訊安全整體應變與防護能力。

參考文獻

1. CVE官方統計資料 (https://www.cve.org/about/Metrics)
2. CISA官方網站 (https://www.cisa.gov/)
3. CISA KEV公告清單 (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
4. CISA KEV說明文件 (https://www.cisa.gov/known-exploited-vulnerabilities)
5. CWE 官方網站 (https://cwe.mitre.org/)
6. CVSS 說明文件 (https://www.first.org/cvss/v4.0/implementation-guide)
7. 資安院漏洞示警公告 (https://www.nics.nat.gov.tw/core_business/information_security_information_sharing/Vulnerability_Alerts/)
8. 國家資安資訊分享與分析中心介紹 (https://www.nics.nat.gov.tw/core_business/information_security_information_sharing/National_Cyber_Security_Information_Sharing_and_Analysis_Center/)

關鍵字：CISA KEV、漏洞分析、趨勢

刊　　名　資安週報第 58 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