

資通安全網路月報

一、資安長話短說

對兩個機關使用同樣的攻擊手法，一個能及時發現應處，另一個卻直到全面淪陷都未能察覺，一場真實紅隊演練告訴我們：偵測工具再好，當工具背後的制度、流程與人員無法相互配合運作時，告警也只是被淹沒的雜訊。

(一) 結果兩極的紅隊演練

美國網路安全暨基礎設施安全局 (Cybersecurity and Infrastructure Security Agency, CISA) 於 115 年 8 月公開一份紅隊演練評估報告^註，CISA 挑選兩個關鍵基礎設施機構 (以下分稱 A、B 機構)，運用相同攻擊手法，兩者結果卻大相逕庭，A 機構被紅隊取得網域最高權限，並可存取機敏業務系統，甚至被潛入資安監控中心 (Security Operations Center, SOC) 作業人員信箱內確認是否監控到已被入侵，全程未遭到任何攔阻；B 機構卻在紅隊執行操作後的幾分鐘內，完成偵測與隔離。這場演練揭示網路安全防禦的領域中，威脅偵測並不是僅依賴資安工具就好，更重要的是機構人員看得懂告警、判斷得出風險、有權限立即採取行動，否則也只是用資安工具所堆疊出來的脆弱城牆。

(二) 差異從何而來？不在採購清單上的三個關鍵

1. 過多的告警資訊，導致難以看見真正的威脅

演練過程

事實上，A 機構已部署多項端點偵測與回應(Endpoint Detection and Response, EDR) 等監控工具，但因未建立明確的正常行為基準，例如員工帳號通常從哪些 IP、在什麼時段登入、哪些端點設備間會互相連線、哪些應用程式會呼叫哪些 API 等，使 SOC 接收大量日常業務活動相關之數千筆誤判警訊，產生「告警疲勞」卻又沒有調整告警規則來篩選過濾，所以紅隊所觸發中、低等級告警遭到忽略而未獲得適當調查與處置。反觀 B 機構因建立了適當的告警規則與設定過濾條件機制，包含針對「異常登入特徵」及「可疑 API 流量」建置自動化告警機制等，使 SOC 人員於接獲告警後，即可迅速採取處置行動。

建議作為

建議各機關(構) 針對偵測機制建立正常行為基準，依實際業務環境持續優化規則、嚴重性分級與告警門檻，讓真正威脅行為能被即時辨識及處理，使資安偵測工具從「有部署」轉化為「能發現、會判斷、可處置」，避免重要威脅情資淹沒在告警之中。

2. 看到告警還不夠，必須讓「看到的人」有權處理

演練過程

資安監控工具發出告警，並不代表機構就具備即時應變處置能力，例如這場紅隊演練中，紅隊曾觸發 A 機構某一伺服器告警，SOC 人員已有發現，但因不同 SOC 團隊間資訊未整合，亦缺乏所管系統的完整資訊，致無法確認系統負責人、系統功能及正常使用情境，最後將告警判定為誤報結案，顯示 A 機構內各部門間缺乏溝通及資訊共享機制，又事件處置權責與授權機制不清，即使監控工具已發送告警訊息，但因為沒有連繫至系統負責人或具決策權人員的管道，只能將風險告警判斷為誤報，錯失處理時機，直至機構全面受駭也毫不知情。相較之下，B 機構則因賦予 SOC 人員適當的處置權限，讓人員能在確認告警內容後，於 20 分鐘內直接隔離 3 部受駭主

機，即使後續紅隊嘗試攻擊營運技術（OT）網路時，也因異常活動再次觸發告警，旋遭 SOC 人員即時管制對外連線及隔離主機。

建議作為

建議各機關（構）建置跨部門與 SOC 間的標準溝通與通報機制，明確定義各部門事件處置權責與通報窗口，確認告警出現後「誰負責判斷、誰有權處置、如何通報升級」，並授權 SOC 人員於事件發生當下，可即時採取必要行動的權限，如直接採取主機隔離、帳號封鎖或網路阻斷等措施，同時建立事後通報與紀錄機制，讓處置過程留下軌跡，以確保第一時間即遏止威脅擴散，讓「發現告警」進化為「控制事件」。

3. 存取控制不能只關注「真人使用者」

演練過程

回到開頭那一幕，紅隊之所以能讀取 A 機構 SOC 人員的信箱，靠的不是某個人的帳號密碼，而是一個可讀取全機構電子郵件的雲端應用程式，然而，過去並未探討過為什麼該雲端應用程式需要這個權限。在這場紅隊演練案例中，兩個機構雖然在端點偵測與應變能力上有所差異，但兩者在雲端環境均因類似的身分治理與權限控管漏洞而遭到紅隊入侵成功，背後關鍵在於許多機構在身分與存取管理上，習慣以「人」為主要管理對象，卻容易忽略同樣具有存取系統與資料權限的應用程式、服務帳號及各類存取憑證等「非人類身分」（Non-Human Identities，NHI）的管理。雲端環境的資安防護不能只問「誰可以登入」，更要掌握「什麼程式可以存取、存取權限有多大，以及發生異常時能否立即收回權限」等控制措施。

建議作為

建議各機關（構）重新盤點應用程式、服務帳號及存取憑證之權限，落實「最小權限原則」及建立憑證、存取金鑰等的生命週期管理機制；此外，制定雲端環境遭入侵的應變標準作業流程，當發生異常時，可迅速停用帳號、撤銷存取憑證等。將平時僅「管好真人使用者」進一步做到「管好非人類身分」。

（三）給資安長的話

綜上，依美國 CISA 紅隊演練案例，建議資安長可從三個面向主動檢視：

- (1) **工具要會看**：建立正常行為基準，持續調校告警規則，避免重要威脅淹沒在大量告警中。
- (2) **機制要會動**：明確定義 SOC 及相關單位權責，授權必要的隔離、封鎖等處置措施，確保發現異常後能立即行動。
- (3) **權限要會管**：落實最小權限與雲端存取控管，除管理真人使用者帳號外，也要納管應用程式、服務帳號及存取憑證等非人類身分帳號。

註：[Cybersecurity and Infrastructure Security Agency \(CISA\), "A Tale of Two SOC's: Insights From Two Red Team Assessments," Cybersecurity Advisory AA26-237A, August 25, 2026](#)

二、資安政策及宣導

（一）發布《政府因應先進 AI 資安風險政策》，因應先進 AI 資安新挑戰

因應先進 AI 降低攻擊門檻、加速漏洞遭惡意利用等新興威脅，數位發展部資通安全署於 9 月 4 日發布《政府因應先進 AI 資安風險政策》，以

「加速防禦、提升資通訊產品安全、強化國家資安韌性」為政策主軸，分短、中、長期推動各項因應策略：

1. 短期策略 - 加速防禦，降低當前曝險：優先調整既有機制並導入可即時運用的防禦工具，縮短資安漏洞發現、影響研判至完成處置的時間。
2. 中期策略 - 提升資通訊產品與供應鏈安全：將治理範圍延伸至產品與供應鏈，從政府採購、產品安全及供應商管理等面向，逐步落實安全設計理念。
3. 長期策略 - 深化國際合作，建立自主 AI 資安防禦能力：積極爭取使用國際先進 AI 模型，並強化重大威脅情資分享機制，及結合產官學研跨界協作，建構我國自主 AI 資安防護能力。

（二）發布《電子看板資通安全管理須知》，守護公務場域資訊安全

數位發展部資通安全署於 9 月 16 日發布《電子看板資通安全管理須知》，提醒各公務機關落實「網段區隔及防禦」、「建立內容發布機制」、「委外及供應鏈管理」及「即時阻斷錯假訊息」等措施，亦鼓勵公有場域委外營運業者及特定非公務機關參考須知深化自主管理，以協助各界提升資安韌性與防護能力。

三、近期資安事件分享

（一）API 存取資料未落實身分驗證，恐致個資外洩

近期發現某機關網站與後端系統交換資料的應用程式介面（Application Programming Interface，API）有存取控制管理缺失。該 API 主要提供會員資料查詢功能，使用者只要輸入會員編號，系統便會回傳對應會員的身分證字號、姓名、電話及電子郵件等個人資料。

造成個資外洩漏洞的關鍵問題在於，系統未先行確認使用者是否已登入成功，也未進一步驗證其是否具備查閱該筆資料的權限；因此，攻擊者

不必依循網站正常操作流程，只要直接呼叫 API，並依序變更會員編號，即可能逐筆取得其他會員的個人資料，形成大規模資料外洩風險。

此案例顯示，API 雖是系統間資料交換的重要管道，但若缺乏完善的身分驗證與權限控管，即可能成為資料外洩的漏洞。除確認「能不能登入」外，更應進一步確認「可以存取哪些資料」，落實 API 的身分驗證、最小權限原則及安全邊界。

（二）經驗學習（Lessons Learned）

近期攻擊者頻繁針對網站 API 進行探測與利用，API 係設計供系統或程式直接交換資料使用，請求與回傳格式多為固定，可直接利用系統既有功能取得結構化資料。因此，攻擊者一旦掌握 API 路徑與使用方式，便可透過自動化程式（如爬蟲程式）持續呼叫，以利大量蒐集資料。一旦 API 的身分驗證或存取控制存在漏洞，攻擊者甚至無須入侵資料庫，即可能利用系統既有 API 功能取得未經授權之資料，擴大資料竊取範圍，有鑑於此，建議各機關應落實以下防護措施：

1. **落實後端身分驗證與存取權限檢查：**考量攻擊者可以繞過網頁介面檢核，直接呼叫 API，故涉及個人資料或非公開業務資訊之 API，勿僅於前端介面進行權限控管，而是應於後端確實驗證使用者身分，並依「最小權限原則」檢核使用者角色、業務權限及資料歸屬，確認是否有權存取資料及可以存取什麼資料；也需防範使用者透過變更 API 請求中的 ID、案件編號或其他識別值，來取得其無權存取之其他使用者資料之風險。
2. **妥善管理 API 金鑰憑證：**對於以 API 金鑰（API Key）作為存取憑證之 API，應依「最小權限原則」為其設定適當的存取權限與使用範圍，避免所有 API 共用相同金鑰或使用具過度權限的金鑰。API Key 不應直接寫入前端程式碼、公開程式碼庫或其他容易遭取得的位置，並應建立金鑰生命週期管理機制，包括定期更換、停用及撤銷。倘發現 API Key 遭駭外洩，應能即時撤銷並重新產製，降低遭入侵之受損範圍。

3. **採用隨機識別碼降低列舉風險**：API 所使用之資源識別碼，如使用者 ID、案件編號或其他物件識別值，應避免採用容易猜測、具規律性或連續遞增之編號，可參考 OWASP 相關指引，採用難以預測之隨機識別碼或通用唯一識別碼，降低遭攻擊者大量猜測與自動化列舉之風險，惟該作為僅屬降低風險的輔助措施，不可取代後端實質的身分驗證及權限檢查。
4. **限制 API 回傳資料範圍**：API 應依實際業務需求採取「資料最小化」原則，僅回傳必要欄位，避免一次提供過多非必要業務資料；對於不同角色或使用情境，亦應依權限提供適當之資料欄位及資料範圍，尤其，針對敏感或高風險資料，應採取遮罩、部分揭露等措施，以降低資料暴露程度。
5. **實施 API 請求頻率及流量限制**：應依 API 的業務特性設定適當的請求頻率、流量或數量限制，必要時針對使用者、帳號、來源 IP 或 API Key 等建立控管機制，避免攻擊者透過自動化程式持續呼叫 API，大量蒐集資料，造成機敏資料外洩。對於短時間內大量查詢等異常行為，應建立適當的阻擋或告警機制。

參考資料：《資通安全責任等級分級辦法》- 附表十 - 資通系統防護基準 - 存取控制及系統與資訊完整性

四、資通安全趨勢

（一）事前聯防監控

1. 監控情資統計

本月蒐整政府機關資安聯防情資共 9 萬 1,731 件(增加 1 萬 4,014 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類 (59%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類 (21%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類 (8%)，大多是系統遭未經授權存取或取得系統/使用者權限。統計近 1 年情資數量分布，詳見圖 1。

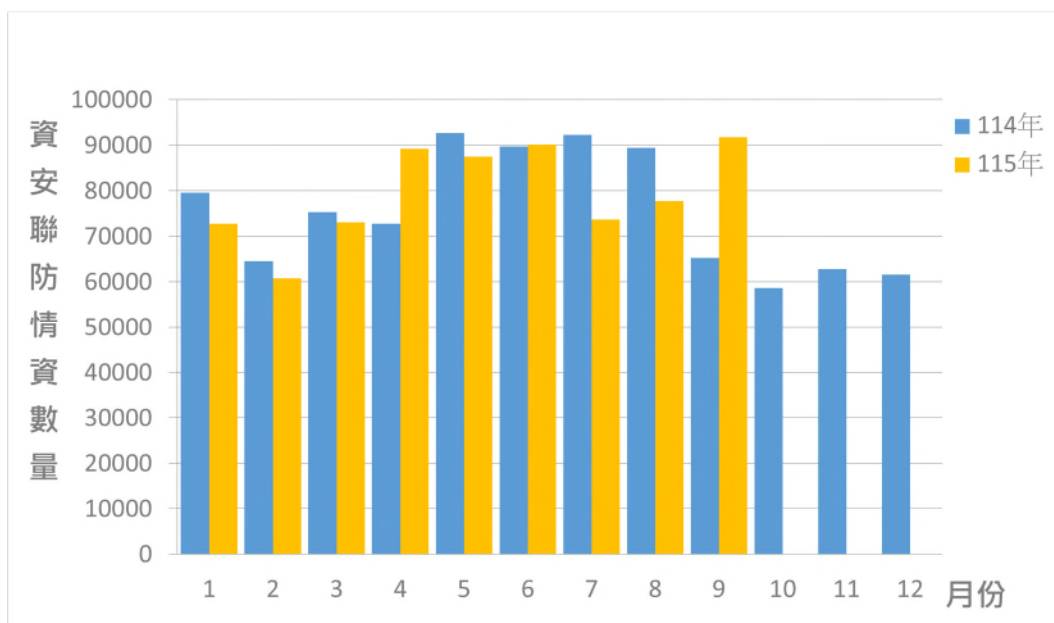


圖 1 資安聯防監控情資統計

2. 本月情資分析：駭客透過惡意郵件植入木馬，竊取機敏資訊

經進一步彙整分析聯防情資資訊，發現近期駭客透過惡意郵件散布 ValleyRAT，以竊取電腦機敏資訊。ValleyRAT 是一種遠端存取木馬，其具備鍵盤側錄、螢幕擷取、檔案及敏感資訊竊取等功能，駭客可遠端控制受感染主機，亦可依駭客指令下載及執行其他惡意模組，進一步擴大受駭主機遭入侵之影響，相關情資已提供各機關聯防監控防護建議。

(二) 事中通報應變

本月資安事件通報數量共 204 件（包含攻防演練數量 95 件），為去年同期的 1.94 倍，通報類型以非法入侵為主，占本月通報件數 50.98%。本月發現部分機關因網站 API 缺乏完善的身分驗證與存取控制機制，導致非公開資料遭未授權存取而外洩。近 1 年資安事件通報統計詳見圖 2。

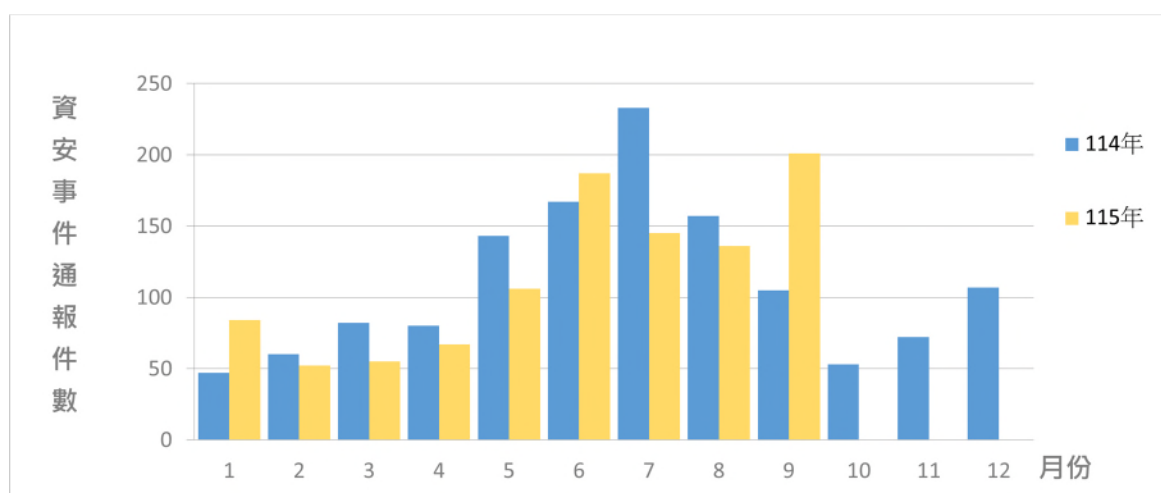


圖 2 資安事件通報統計

五、國際資安新聞

(一) 輝達 NemoClaw 出現漏洞，惡意網站可劫持 OpenClaw AI 代理人

(資料來源：[Hack Read](#))

NVIDIA (輝達) NemoClaw 為部署 OpenClaw AI Agent 的工具，透過 OpenShell 沙箱限制 Agent 對主機環境的存取，並搭配 Ollama 在本機執行 AI 模型。然而，資安公司 Oasis Identity Research 揭露該工具存在 CVE-2026-65105 漏洞，該漏洞可讓攻擊者在使用者造訪惡意網頁之後，以未經身分驗證方式存取本機 Ollama 模型伺服器，雖然 Ollama 可透過瀏覽器來源檢查 (browser-originchecks) 及 Host 標頭驗證 (Host header validation) 限制遠端網站存取本地服務，但攻擊者透過 DNS 重綁定 (DNS rebinding) 技術可繞過來源檢查，使瀏覽器在不需身分驗證的情況下取得受害者本機的 Ollama API 存取權，進而執行、下載或刪除模型，及讀取或修改模型範本與系統提示詞 (system prompts)，並利用受害者的 GPU 執行模型推論，且同一區域網路內的其他裝置亦可能直接存取該 API。此外，

攻擊者可修改模型的聊天範本 (ChatTemplate)，植入隱藏指令，使惡意內容持續影響後續對話及 AI Agent 運作 (截至最初揭露時，尚未發現實際攻擊利用證據；NVIDIA 後續已發布安全性更新)。

(二) 美國指稱部分中國 AI 企業非法蒸餾模型

(資料來源：[Bank Info Security](#))

美國網路安全暨基礎設施安全局 (CISA)、國家安全局 (NSA) 與聯邦調查局 (FBI) 於 2026 年 9 月 8 日聯合發布警訊，指稱 DeepSeek、月之暗面 (Moonshot AI) 及阿里巴巴等部分中國 AI 企業，自 2024 年起透過中轉代理伺服器方式，繞過地理限制與安全機制，並分散於不同平台以降低被偵測的風險，再利用 API 對美國先進 AI 模型，包括 Anthropic 的 Claude、OpenAI 的 GPT、Google 的 Gemini 以及 xAI 的 Grok 進行數百萬次互動與請求，取得數十億個「詞元」 (Token)，提取模型的推理、軟體工程能力，進行「模型蒸餾」以用於訓練自有模型。

美方表示，此類行為不僅會造成重大經濟損失與專有技術洩漏，更會削弱美企競爭優勢，相關機構敦促產業針對疑似模型蒸餾行為，應強化偵測應對機制，並建立跨組織情資共享以積極防範。

(三) Google 發布警告：Chrome 出現已遭利用於攻擊的新零日漏洞

(資料來源：[Bleeping Computer](#))

Google 於 9 月 8 日發布 Chrome 153 穩定版更新，修補 230 項安全性問題，其中包括已遭實際利用的高風險零日漏洞 CVE-2026-87491。該漏洞由首爾大學 Compsec Lab 研究實習生 Jihyeon Jeong 通報，源於 Chrome 的 V8 JavaScript 與 WebAssembly 引擎的越界寫入 (out-of-bounds write) 缺陷。遠端攻擊者可透過特製 HTML 頁面利用該漏洞，在 Chrome 沙盒內執行任意程式碼；漏洞的利用亦可能造成堆積記憶體損壞 (heap corruption)，使攻擊者存取超出記憶體緩衝區的資料，進而導致

敏感資訊洩露或瀏覽器當機。

Google 已針對 Windows、Mac 和 Linux 發布桌面穩定版更新 (Chrome Desktop Stable Channel Update)，由於全球推送可能耗時數天至數週，且該漏洞已出現實際攻擊情形，建議使用者立即手動更新或重新啟動 Chrome 以完成套用，以降低遭受攻擊的風險。

參考附錄-本月重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	應用程式伺服器 Oracle WebLogic Server 嚴重程度： CVE-2026-83021： CVSS v3.1 10.0 CVE-2026-83038： CVSS v3.1 9.9	● Oracle WebLogic Server 之 Web Container 與 TopLink Integration 元件存在重大安全漏洞 (CVE-2026-83021、CVE-2026-83038)。 ● 前者可由未經身分鑑別之遠端攻擊者透過 HTTP 攻擊接管伺服器；後者則為具低權限的攻擊者可透過 HTTP 入侵伺服器，可影響系統機密性、完整性及可用性。 ● <u>官方已發布 115 年 9 月安全性修補更新，建議依所用 WebLogic 版本及公告之修補對照表，儘速採取適用更新。</u>
	郵件安全設備 Cisco Secure Email Gateway / Secure Email and Web Manager 嚴重程度： CVE-2026-76440： CVSS v3.1 9.8) CVE-2026-76441： CVSS v3.1 9.8 CVE-2026-20353： CVSS v3.1 9.8 CVE-2026-76443： CVSS v3.1 9.8	● Cisco 郵件安全閘道及集中管理系統存在多項安全漏洞，涉及檔案存取、身分驗證、權限控管及輸入資料處理等功能。 ● 其中部分漏洞可由未登入系統的遠端攻擊者利用，可能造成敏感資料外洩、資料遭竄改或設備服務中斷。 ● <u>官方已釋出修補版本：SEG 請更新至 15.5.5-014 或 16.5.0-780；SEWM 請更新至 15.5.5-006 或 16.5.0-429，或各分支後續修正版；16.0 分支請遷移至修正版。</u>

警訊	類別	內容說明
	行動裝置管理系統 Ivanti Endpoint Manager Mobile (EPMM) 嚴重程度： CVE-2026-18851： CVSS v3.1 8.8	- Ivanti Endpoint Manager Mobile 存在缺少授權檢查漏洞(CVE-2026-18851)。 - 已通過身分鑑別之遠端攻擊者可利用此漏洞將自身權限提升至管理員權限，影響集中管理之裝置管理環境。 - 官方已提供修補版本，建議依使用分支更新至 12.10.0.0、12.9.0.2、12.8.0.4 或後續修正版。
已知遭駭客利用之漏洞	企業開發平台 GitLab CE / EE 嚴重程度： CVE-2026-85706： CVSS v3.1 10.0 CVE-2026-87719： CVSS v3.1 9.9	- GitLab 存在路徑遍歷及不安全反序列化漏洞。CISA 於 9 月 11 日將 CVE-2026-85706 列入 KEV。 - 前者於特定條件下可使未經身分鑑別之攻擊者讀取伺服器任意檔案；後者須為具 Duo Chat 存取權之已驗證使用者，可取得 Advanced Search 設定與敏感憑證。 - 官方已提供修補，建議依官方公告，針對使用中的產品版本套用安全性更新。
	防火牆與 VPN 設備 Check Point Security Gateway / Spark Firewall 嚴重程度： CVE-2026-85102： CVSS v3.1 9.8	- Check Point VPN 協商流程存在不當憑證驗證漏洞 (CVE-2026-85102)，CISA 於 9 月 22 日列入 KEV，原廠亦確認觀察到利用情形。 - 於使用站對站 VPN 或遠端存取 VPN 之受影響設備，未經身分鑑別之遠端攻擊者可利用憑證處理缺陷執行任意程式碼。 - 官方已提供修補，建議依原廠公告，針對使用中的產品版本套用安全性更新。

警訊	類別	內容說明
	應用交付與 VPN 設備 Citrix NetScaler ADC / Gateway 嚴重程度： CVE-2026-88771： CVSS v3.1 9.8) (CVE-2026-88772： CVSS v3.1 8.1	● Citrix NetScaler 存在輸入驗證及記憶體溢位漏洞 (CVE-2026-88771 、 CVE-2026-88772)，CISA 於 9 月 27 日列入 KEV，Citrix 亦確認已遭利用。 ● 前者可使未經身分鑑別之攻擊者執行任意命令，包含預設組態；後者須啟用 DTLS，可能造成遠端程式碼執行或阻斷服務。 ● 官方已提供修補，建議依原廠公告，針對使用中的產品版本套用安全性更新。
	企業協作平台 Microsoft SharePoint Server 嚴重程度： CVE-2026-65660： CVSS v3.1 8.8	● Microsoft SharePoint 存在程式碼注入漏洞(CVE-2026-65660)，CISA 於 9 月 25 日列入 KEV。 ● 已通過身分鑑別之遠端攻擊者可利用此程式碼注入漏洞透過網路執行程式碼，影響 SharePoint 伺服器安全。 ● 官方已提供安全更新，請依 SharePoint 版本確認並套用包含本漏洞修補之更新。

警訊說明：

「漏洞警訊」：為已驗證漏洞但尚未遭攻擊者大量利用，修補速度建議儘快安排更新。

「已知遭駭客利用之漏洞」：已知有漏洞成功攻擊情形，建議即刻評估修補。