資通安全網路月報

一、資安長話短說

（一） 當遭受攻擊致組織難以運作時，怎麼辦？

身為資安長的您，想像某天突然收到各部門主管慌亂地報告系統遭受網路攻擊，關鍵服務幾近停擺，面對鋪天蓋地的混亂，與來自內、外部的高度壓力，此時該如何應對？

面對網路攻擊，機關容易產生「不惜代價儘快修復」或「立即追究責任」的直覺反應。然而在資訊不足及高度壓力的情況下，倉促決策反而可能增加復原的困難，為此，英國國家網路安全中心（National Cyber Security Centre，NCSC）於 115 年 7 月 28 日發布「遭網路攻擊該怎麼辦」應變指南[註 1]，將復原作業劃分為三個核心階段：**「立即行動」➔「復原與調查」➔「重建」**，並列舉對應的應對措施，協助機關有序完成復原作業。

（二） 三個應對階段：解析英國應變指南背後的核心思維

1. 階段一：立即行動（最初幾個小時）—保持冷靜，穩住局勢

資安事件發生的最初階段，正是機關陷入極度混亂與充滿焦慮的情境，

因此，一開始必須以冷靜及專業的態度，掌握「發生了什麼、影響多大、接下來誰負責，以及是否尋求外部支援」等相關資訊，阻止災情繼續擴大。

(1) 用「權責明確的指揮結構」取代「多頭決策的集體焦慮」：

當業務全面停擺，訊息混亂的狀況下，最怕變成「大家一起處理，卻沒人知道誰決定」的亂象。因此第一時間啟動既有的事件指揮機制，將職責適度指派，明確分配決策、技術處理、營運應變及公關溝通的責任邊界，避免各自為政，並確保訊息傳遞順暢，讓整體應變行動有條不紊地進行，阻止損害繼續擴大。

(2) 「關機」與「斷網」是多維度風險管理的決策權衡：

發現系統被駭，要選擇關機？還是斷網？往往是第一個面臨的決策，緊急關閉系統雖可快速中止正在執行的惡意活動，卻可能讓部分重要鑑識證據消失，也無法進行攻擊者入侵的根因分析，進而大幅提升後續再次受駭（Re-compromise）的風險；而中斷受駭系統的網路連線，可阻止攻擊者持續遠端控制受駭設備，也降低威脅擴散的風險，但可能無法中止系統內部已經被觸發、暗中執行的惡意程序。因此，身為資安長的您必須扮演「風險衡平者」角色，根據當下威脅擴散急迫性、營運影響與後續資安事件調查等相關因素，權衡評估該關機還是斷網，必要時亦可尋求外部網路事件應變專家協助判斷。

2. 階段二：復原與調查（最初幾天～幾週）—調配有限資源，確保最低可行營運

在最初的數小時緊急混亂被逐漸控制後，目標將轉向循序恢復關鍵的營運服務，必要時可搭配替代方案，讓機關恢復到「最低可行營運（Minimum Viable Operations, MVO）」狀態。

(1) 打破部門本位主義：以「業務需求」制定復原優先序

在復原階段，每個部門可能會強調自己的系統最重要、必須第一個復原，此時資安長需引領各業務部門打破部門藩籬限制，決定復原之業務優先序位必須以「關鍵業務存續需求」與「營運衝擊分析（BIA）」為導向，而非由 IT 技術視角，或僅由系統規模、系統相依性考量。另在有限的資源與時間下，透過暫時性的離線替代方案，讓機關迅速復原到最低可行營運狀態，避免業務徹底停擺。

(2) 復原工作避免急於求成，防範二次受駭風險：

在遭受網路攻擊後，機關往往面臨來自內、外部壓力，導致容易落入急於求成的情形。然而，若在未確認攻擊者入侵途徑已遭阻斷、且惡意活動已被完全根除前，貿然復原系統極可能導致二次資安事件的發生。其中目錄服務（AD）為各項應用服務之基礎架構，考量攻擊者可能早已潛伏掌控部分帳號或新增未授權的特權帳號，復原

過程建議優先聚焦於重新建構可信任的身分驗證機制，以防範二次受駭風險。

(3) 疲勞倦怠的危機管理—別讓員工面臨崩潰臨界點：

網路攻擊復原作業不是百米衝刺競賽，而是一場考驗機關續航力的馬拉松，建議資安長應關注員工在高壓下的身心狀況，除與員工保持通暢、公開的溝通管道、照顧員工的心理狀態，及實施輪班制度外，當內部員工疲憊不堪或能力不足時，亦可透過臨時增援措施或尋求外部專業事件應變團隊協處，以緩解事件發生時員工的工作負荷，及避免影響復原作業。

3. 階段三：重建（未來幾個月內）—化危機為機關未來的防禦韌性

(1) 讓同仁休養生息，而非僅是重建系統：

員工是機關韌性的重要一環，重大資安事件後，第一線技術團隊往往已面臨嚴重的身心透支，「修復同仁」與重建系統同等重要，建議主動為同仁提供休養與調適機制，不僅是人本關懷，更是事件後防範關鍵資安人才流失、恢復士氣，進而確保機關穩健回歸常態營運的關鍵決策。

(2) 根因分析及分享經驗：

需從資安事件中發掘根因，及持續改善機關的資安弱點，並鼓勵分享經驗學習，且將經驗轉化為未來的資安防護與強化韌性計畫，但也要

切忌在機關未完全復原穩定前就嘗試全面轉型，避免延緩業務復原的時程，並給早已疲憊的機關帶來二次負擔。

（三） 給資安長的話

NCSC 的應變指南為機關遭遇網路攻擊時，提供一套從初期識別、損害控制、內外部溝通，到系統復原與事後檢討的實務指引，與我國數位發展部資通安全署 115 年 7 月 31 日發布的《資安事件應變處理行動指引》之精神不謀而合，皆著重於建立完整的緊急應變流程。

資安事件考驗的不只是技術能力，還包括在充滿壓力與不確定性的情境下，機關能否展現韌性？真正具備韌性的機關，不在於從不遭遇危機，而是在面對危機時，能夠冷靜判斷、快速應變及穩健復原，並將經驗轉化為改善制度、技術與營運面，經由這個過程讓機關更加強韌！

註 1：**What to do when cyber attacks disrupt your organization ,28 July 2026,** https://www.ncsc.gov.uk/collection/what-to-do-when-cyber-attacks-disrupt-your-organisation

二、資安政策及宣導

各機關（構）應強化資安管理網通設備及物聯網設備對外連結

為降低各機關（構）網通設備及物聯網（Internet of Things， IoT）設備因遭駭利用作為入侵管道之風險，數位發展部資通安全署建請各機關（構）辦理以下事項：

1. 須全面盤點資產清冊及指定管理權責，並應自網際網路側檢視自身對外可見情形。
2. 嚴禁將網通及 IoT 設備管理介面直接曝露於網際網路，應透過虛擬私人網路（Virtual Private Network，VPN）或採用零信任機制進行遠端存取。
3. 應落實最小開放原則，關閉不必要之服務及通訊埠，對必須開放之服務，應停用已知不安全或未加密之通訊協定（如 Telnet、FTP、SNMP v1/v2c 等），並改採用加密安全方案（如 SSH、SFTP、SNMPv3 等）。
4. 定期更新設備韌體並更換密碼為高強度，並訂定漏洞修補時程及管理帳號建議啟用多因子驗證；另針對已終止支援、無法取得安全更新之設備應訂定汰換期程。
5. 採購網通及 IoT 設備時，應將資安要求（如設備具備安全更新機制及可停用遠端連線功能等）納入採購規範。

6. 針對 IoT 設備，建議置於獨立網段隔離，限制其對外連線行為。

7. 公務機關嚴禁下載、安裝或使用危害國家資通安全產品

上述落實作為及委外活動網站網域管理情形，將納入後續行政院資通安全稽核之稽核項目。

三、近期資安事件分享

設備交接未完整，漏洞管理未落實

某機關因轄區遼闊，故多處設立監視器並建置監視系統，且於系統前端設置防火牆以提升安全防護能力。惟近期接獲資安警訊通知，發現有可疑連線行為，經確認防火牆遭駭客入侵並取得控制權，竄改最高管理者帳號與密碼，及利用該設備連線至機關內部網路，造成資安威脅。

經追查發現，本案主要發生原因為設備交接程序及後續資產盤點未臻完善所致，本案於辦理業務移轉時，僅完成書面文件移交作業，但未同步確認設備的詳細狀況（例如現在使用版本、原廠維護狀態、設備使用年限及預計汰換時限等資訊），交接程序不完整。

同時，業務接手單位承接業務後，亦未落實資產盤點及持續追蹤設備維護與汰換狀況，以致未掌握該防火牆的使用年限和原廠支援狀況，導致設備在超過原廠支援期限（EOS）後仍持續使用，因持續未取得最新的官方安全性更新或修補程式，最終因出現漏洞而遭駭客入侵取得防火牆的管

理權限，竄改了最高管理者帳號與密碼，進一步連線至機關內部網路，嚴重影響機關整體資通安全。

經驗學習（Lessons Learned）

本案核心問題非單純在於設備過於老舊，而是在業務移轉後未掌握設備現況與落實生命週期管理，導致原本應作為資安第一道防線的設備長期處於資安防護盲區，形成破口。為避免類似情形再次發生，建議各機關應落實以下防護措施：

（一）設備交接確實做好資安體檢

1. **落實設備現況清查**：機關進行組織調整或業務移轉時，除清點硬體數量及基本資料外，也應確認設備使用版本、更新及修補狀況、原廠支援期限（EOS / EOL）及維運合約等，全面掌握設備實際防護狀態。
2. **釐清維護權責與合約狀態**：交接時應確認設備是否在原廠支援或維護合約效期內，並釐清後續維護責任與經費來源，視設備現況預先規劃汰換時程，避免設備移轉後出現管理責任不明或維護中斷的情形。

（二）IoT 設備存取管理：

1. **避免管理介面直接暴露於網際網路：**監視器、防火牆等 IoT 設備之管理介面，原則上不應直接開放網際網路進行遠端存取，以降低遭外部攻擊的風險。
2. **落實獨立網段隔離：**應將 IoT 設備管理介面與資料傳輸網段進行實體

或邏輯隔離，透過存取控制，一旦設備遭駭後，有效阻斷駭客進一步向機關內網進行橫向移動（Lateral Movement）的攻擊風險。

3. **強化遠端維運存取控制：**若有管理需求，應以現場維護為優先，遠端連線則應以「原則禁止、例外允許」為原則。如必需開放遠端連線管理，應以「短天期」為限，權限為臨時性，用完即關閉，並採用零信任及來源 IP 白名單、異常行為監控管理等機制，以提升資安防護安全性。

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

本月蒐整政府機關資安聯防情資共 7 萬 7,717 件(增加 4,067 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(55%)，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(24%)，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。

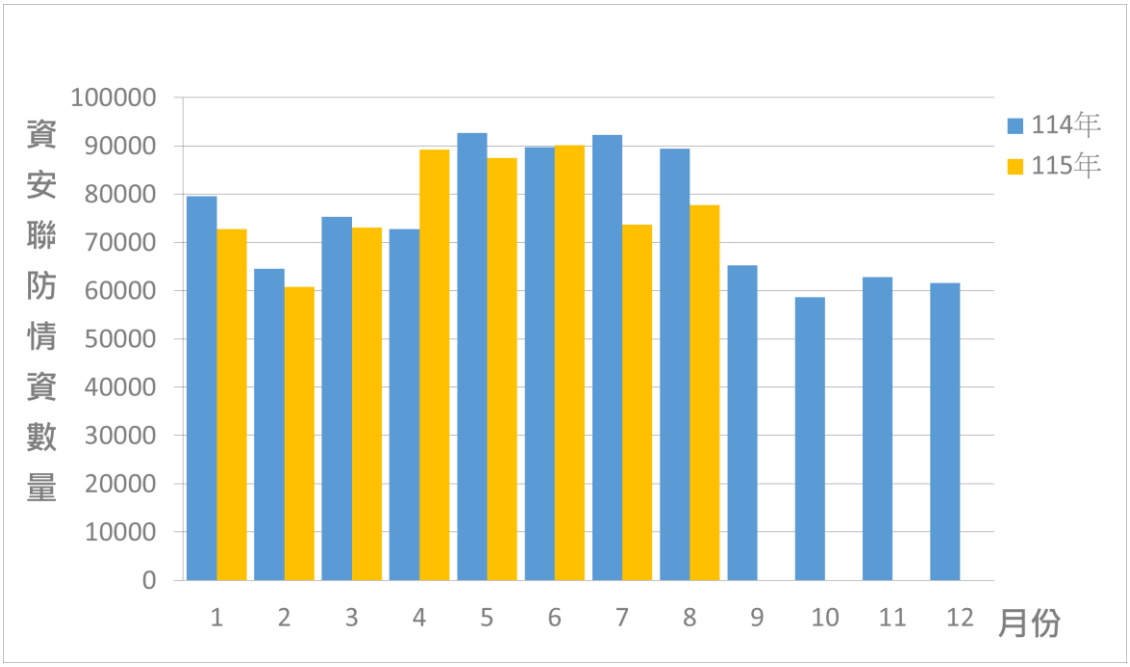

圖 1　資安聯防監控情資統計

駭客透過惡意郵件竊取電腦機敏資訊

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 XWorm 以竊取電腦機敏資訊，XWorm 是一種資訊竊取遠端操控木馬，具備遠端控制、鍵盤側錄、螢幕擷取及敏感資訊竊取，除了竊取敏感資訊外，亦具備下載後續更多惡意程式之功能。此次駭客利用付款通知與款項入帳等財務議題進行社交工程誘騙，使用包含惡意 JavaScript 腳本檔案之壓縮檔作為附件，企圖誘騙收件人點選執行惡意 JavaScript 腳本以觸發後續惡意程式，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 136 件（包含攻防演練數量 55 件），為去年同期的 0.87 倍，通報類型以非法入侵為主，占本月通報件數 47.06%。本月發現部分對外連網設備及網站服務仍存在安全控制不足情形，包括設

備漏洞未修補、管理介面暴露及使用預設帳號密碼，輸入驗證及存取權限控管不足等，導致可能遭利用漏洞或 SQL Injection、目錄遍歷及 API 權限控管缺失等方式嘗試取得網站資料。近 1 年資安事件通報統計詳見圖 2。

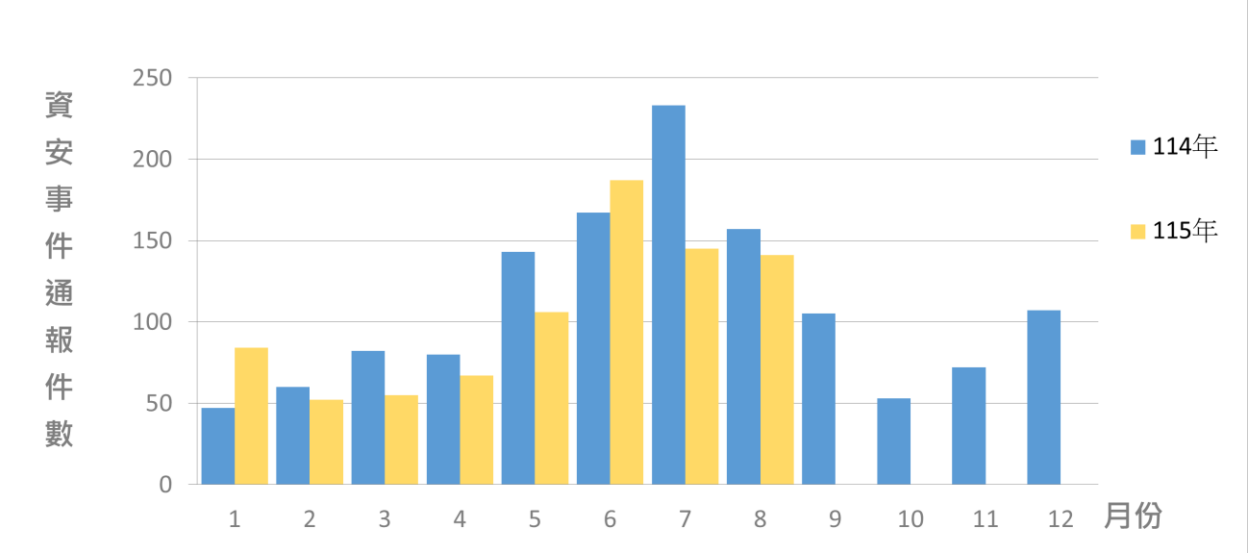

圖 2　資安事件通報統計

五、國際資安新聞

CISA 給予聯邦機構 3 天時間修復已遭積極利用的 Ray RCE 漏洞

（資料來源：The Register）

美國網路安全暨基礎設施安全局（CISA）報告指出，CVE-2025-62593（CVSSv4 評分為 9.4）——一項存在於 Ray 系統（用於擴充 Python 及機器學習工作負載的開源框架）中的嚴重 RCE（遠端程式碼執行）漏洞，該漏洞主要為 2.52.0 之前的 Ray 版本。漏洞源於 Ray 透過檢查網路連線請求中

的 User-Agent 標頭（Header）是否為『Mozilla』，來識別並阻擋來自瀏覽器的連線請求。然而，Firefox 和 Safari 瀏覽器卻允許網頁腳本（JavaScript）利用 Fetch API 去修改這個標頭欄位，一旦開發人員造訪可疑網站或在受影響的瀏覽器中收到惡意廣告，即可能遭到利用，讓攻擊者能夠入侵開發人員的電腦執行任意程式碼，或利用瀏覽器當跳板，攻擊企業私有網路上的 Ray 節點，藉此攻破其他同網段下的 Ray 主機。

Ray2.52.0 已修復此問題，並新增了可選的權杖身分驗證作為額外防禦手段，CISA 強制要求聯邦機構要在 3 天修復該漏洞，而非常見的 14 天。

美國警告：關鍵基礎設施中的西門子 PLC 正遭受人工智慧攻擊

（資料來源：Bleeping Computer）

美國網路安全機構發布一份聯合資安公告，警告駭客正利用 AI 所生成的腳本針對關鍵基礎設施領域中西門子（Siemens）S7 系列可程式邏輯控制器（Programmable Logic Controllers,PLC）進行攻擊，PLC 是工業專用電腦，用於自動化和控制工廠及其他關鍵基礎設施中的機器與實體運作流程。

駭客利用 Censys 與 ZoomEye 等網路掃描工具來定位暴露於網路上的 PLC，並利用人工智慧開發 Python 攻擊腳本，透過 snap7.dll 與 python-snap7 函式庫（libraries），將其偽裝成合法的營運技術（Operational

Technology，OT）監控軟體，透過 S7comm 協定取得對 PLC 記憶體、組態資料及梯形圖（Ladder Logic）程式的讀寫權限。目前駭客的動作似乎聚焦於『長期潛伏與潛在調查』，可能是為日後癱瘓關鍵基礎設施做準備，以西門子 S7-200、S7-300、S7-400、S7-1200 與 S7-1500PLC 為主要攻擊目標，報告建議組織應全面進行 S7 PLC 的資產盤點、安裝最新的安全性更新、並阻隔來自外部網路的直接存取、強化存取控制措施，監控這類設備的異常活動。

參考附錄-本月重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	**企業應用與 ERP 平台** SAP Commerce Cloud、SAP MII 與 SAP NetWeaver **嚴重程度：** CVE-2026-58231：CVSS 10.0 CVE-2026-44772：CVSS 9.9 CVE-2026-34265：CVSS 9.8 CVE-2026-44758：CVSS 9.1	● SAP 於 115 年 8 月安全性更新揭露多項重大漏洞，影響 Commerce Cloud、Manufacturing Integration and Intelligence(MII) 及 NetWeaver / ABAP Platform。 ● 其中 CVE-2026-58231 為 Commerce Cloud(Data Hub Adapter)不當授權漏洞，修補釋出 3 日後已觀察到攻擊嘗試並有 PoC 流出(尚未列入 KEV 清單)，且須重新建置並重新部署始生效；CVE-2026-44772、CVE-2026-44758 為 MII 程式碼注入；CVE-2026-34265 為 NetWeaver AS ABAP 記憶體損壞漏洞，最嚴重可能導致任意程式碼執行或系統受控。 ● 官方已發布 115 年 8 月 Security Patch Day，建議依所使用 SAP 產品儘速套用對應安全性更新。
	工作負載安全防護平台 Cisco Secure Workload **嚴重程度：** CVE-2026-20231：CVSS 9.9 CVE-2026-20315：CVSS 10.0 CVE-2026-20317：CVSS 10.0 CVE-2026-20318：CVSS 9.6 CVE-2026-20319：	● 原廠內部安全檢測發現 Cisco Secure Workload 存在注入、不當存取控制、不當驗證、不當輸入驗證及記憶體緩衝區處理不當等 5 項安全漏洞，其中 4 項為重大(Critical)等級。 ● 未經身分鑑別或已通過身分鑑別之遠端攻擊者可利用漏洞影響系統機密性、完整性或可用性；其中兩項漏洞最高達 CVSS 10.0。 ● 官方已釋出修補版本，建議更新至 Cisco Secure Workload 3.10.9.1 或 4.0.4.16(含)以上版本。

警訊	類別	內容說明
	CVSS 7.5	
	網站應用程式防火牆 Fortinet FortiWeb **嚴重程度：** CVE-2026-26035： CVSS 9.8	● 原廠內部安全檢測發現 Fortinet FortiWeb 存在不當驗證 (Improper Authentication) 漏洞 (CVE-2026-26035)。 ● 設備啟用特定非預設遠端 RADIUS 管理者驗證組態(Wildcard，預設為關閉)時，未經身分鑑別之遠端攻擊者可使用任意帳密登入 GUI 或 CLI，取得管理者權限並控制設備；如無法立即更新，可先停用該 Wildcard 選項為暫行措施。 ● 官方已釋出修補版本，建議更新至 FortiWeb 7.2.13、7.4.12、7.6.7 或 8.0.3(含)以上版本。
已知遭駭客利用之漏洞	**應用程式交付與負載平衡設備** Progress LoadMaster **嚴重程度：** CVE-2026-8037：CVSS 9.8	● CISA 已於 2026 年 8 月 7 日將 CVE-2026-8037 列入 KEV 清單。 ● Progress LoadMaster API 存在作業系統命令注入漏洞，未經身分鑑別之遠端攻擊者可利用未妥善處理的輸入，執行任意系統命令。 ● 官方已釋出修補版本，建議更新至 LoadMaster 7.2.63.2；LTSF 分支請更新至 7.2.54.18(含)以上版本。
	網路防火牆與 VPN 設備 Cisco Secure Firewall ASA 與 Secure Firewall FTD **嚴重程度：** CVE-2026-20349： CVSS 8.6	● CISA 已於 2026 年 8 月 11 日將 CVE-2026-20349 列入 KEV 清單。 ● Remote Access SSL VPN 服務處理 HTTP 請求時存在錯誤檢查不足，未經身分鑑別之遠端攻擊者可發送特製 HTTP 請求使設備非預期重新載入，造成阻斷服務（DoS）。 ● 官方已提供修補版本，建議使用 Cisco Software Checker 確認所用 ASA /

警訊	類別	內容說明
		FTD 分支之 First Fixed 版本並儘速更新。
	虛擬化管理平台 Broadcom VMware vCenter **嚴重程度：** CVE-2026-59310：CVSS 9.8	● CISA 已於 2026 年 8 月 18 日將 CVE-2026-59310 列入 KEV 清單。 ● VMware vCenter 的 Syslog Server 存在路徑遍歷漏洞，已取得 VMware vCenter 網路存取權限之遠端攻擊者可利用該漏洞執行任意程式碼；目前已出現攻擊者藉此植入反向 SSH 工具維持存取之實際案例。 ● 官方已提供修補版本，建議 vCenter 9.1 更新至 9.1.0.0300、9.0 更新至 9.0.2.0100，8.0 更新至 U3k / U2f 或後續版本。
	協作與文件平台 Microsoft Office SharePoint **嚴重程度：** CVE-2026-55040：CVSS 9.1	● CISA 已於 2026 年 8 月 18 日將 CVE-2026-55040 列入 KEV 清單。 ● Microsoft SharePoint 存在弱身分鑑別漏洞，未經授權之遠端攻擊者可透過網路繞過安全性功能；影響版本為 SharePoint Server 2016、2019 與 Subscription Edition。另遠端攻擊者可結合 CVE-2026-55040 和 CVE-2026-63520，針對具風險的 SharePoint 伺服器遠端執行程式碼。 ● Microsoft 已提供安全性更新，建議依 Security Update Guide 儘速套用所使用 SharePoint Server 版本之適用修補程式。

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。