資通安全網路月報

一、資安長話短說

做好基本功，不怕人來攻

先進 AI 降低資安攻擊的技術門檻，也加速系統漏洞搜尋及攻擊腳步，面對新型態攻擊，企業防禦的核心仍是落實資安防護基本功，並確保遭受攻擊後具備復原能力。

（一）AI 改變的是「攻擊速度與成本」，但本質仍是利用系統弱點與權限管理疏失

近期國內、外發生多起利用 AI 技術的資安事件，10 月起南韓金融業遭攻擊者疑似運用開源 AI 工具，探測系統漏洞及程式碼分析，並透過多層跳板隱匿行蹤，入侵金融機構系統，造成逾 47 萬筆客戶個資外洩、約 10 億韓元款項被盜；南韓更是發生 1 名非資訊相關科系出身的駭客，僅自學並利用 AI 程式開發代理及自主滲透測試系統，在短短 40 多天內入侵了 60 家公司，竊取資料進行勒索；另日本多家企業亦接連發生個資外洩事件，包括佐川急便、卡普空及樂天旅遊等，雖然個別事件尚未證實使用 AI 工具，但依日本 GMO 公司所公布最新調查結果，已確認有攻擊者利用 AI 工具鎖定約 20 家日本企業發動攻擊；而我國也接連發生十餘家企業及網路平臺接連受害，累計逾百萬份個資受影響。經初步調查，近半數事件與 AI 攻擊有關，攻擊者多以已知遭利用漏洞（Known Exploited Vulnerabilities Catalog，KEV）進行攻擊；此外，API 成為駭客攻擊熱

區，因為 API 取得大量資料相對容易，且部分 API 具有較高權限，一旦受駭極易造成重大衝擊。

上述案例顯示，AI 不僅降低資安攻擊的技術門檻，也加速漏洞搜尋及攻擊流程，攻擊者也未必需要使用全新的攻擊技術，只要取得有效帳號或掌握可利用的系統弱點，就能進一步入侵系統。因此，AI 改變的是攻擊的速度與成本，卻也讓組織原有的資訊資產管理、漏洞修補及帳號權限控管更加重要，因此，防禦的核心仍是落實資安防護基本功，別讓既有的資安管理缺口成為駭客攻擊的入口。

（二）穩紮資安基本功：縮小攻擊面、做好備份備援

面對日益且快速複雜的攻擊威脅，企業未必需要盲目添購更多防禦工具，而是更應該將資安防護基本功作紮實，重新檢視既有系統是否有管理疏漏，並確認一旦系統遭到破壞時，現有的備份、備援機制能否支撐關鍵業務迅速運作。

1. 縮小攻擊面，從資產盤點與管理做起

從許多資安事件分析可以得見，攻擊者往往並不是利用零日漏洞，而是發現各機關因未落實基本資安防護所造成的破口入侵，包括管理介面暴露於網際網路、使用已停止安全性更新的設備，及已知漏洞卻未及時修補等，因此，資安防禦應從「掌握完整資訊資產」與「落實存取控管」開始做起，關閉不必要的對外服務與連接埠，將後臺管理及測試系統連線存取限縮於加密管道，按風險等級高低排定修補漏洞優先順序，同時嚴密管控使用者與系統程式身分的權限管理。

建議作為

(1) **減少暴露資產：**確實盤點並建立網站、VPN、遠端桌面、NAS、路由器、雲端服務及備用、測試系統等資產清冊並指定負責人；導入外部曝險檢測服務（External Attack Surface Management,

EASM）機制，定期檢視對外開放服務與連接埠，遵循「非必要不對外」原則，關閉非必要服務，限縮後臺管理介面存取，並將管理介面與資料傳輸網段進行實體或邏輯隔離。

(2) **優先修補漏洞：**參考 TWCERT/CC 預警及本署甫於 115 年 11 月 6 日發布之《各機關基於風險導向之弱點處置期限評估指引》，考量漏洞是否已被利用、弱點能否被自動化利用等指標評估處置期限；停止支援的設備應儘速規劃汰換期程，作業系統、網通設備與 NAS 安全性更新，應儘速評估並完成修補，倘有暫時無法修補者，應採用限制連線或隔離網段措施，阻斷入侵後遭橫向移動的風險。

(3) **嚴密帳號管理：**落實「最小權限原則」，遠端連線、電子郵件及管理員帳號優先導入多因子驗證（MFA）或通行密鑰（Passkey）；定期清理閒置帳號，將特權帳號（如管理員帳號）與日常辦公帳號（如收發郵件）分開管理。此外，也應盤點應用程式、服務帳號及存取憑證等「非人類身分」（Non-Human Identities，NHI），定期檢視權限與憑證有效性，發現異常時，立即撤銷。

2. **做好備份備援，確保遭受攻擊後也能盡快復原**

當遭受資安攻擊時，若備份環境與正式系統共用帳號或網段，攻擊者可能同時摧毀原始資料與備份；若備份未涵蓋系統設定、資料庫與雲端資訊，並且未曾實際執行還原測試，恐怕難以在可接受時間內恢復關鍵服務。

因此，業務單位及管理階層務需共同確認關鍵服務的恢復優先順序、容許中斷時間及替代作業方案，並定期驗證備份還原與備援切換，避免遭駭後因缺乏明確的恢復順序及演練經驗導致復原進度遲延。此外，應持續確保偵測工具能辨識異常行為，並透過明確的通報與處置流程，將告警轉化為實際防禦行動。

建議作為

(1) **落實備份 3-2-1 原則，確保重要資料可救回：**採用 3-2-1 備份原則，即保留 3 份資料（1 份原始資料及 2 份備份），使用 2 種不同儲存媒介，且至少 1 份離線或設為不可刪改，以確保即使正式環境遭入侵，備份資料也不會一併被竄改或加密；備份資料範圍並應涵蓋業務資料、資料庫及必要的系統設定。

(2) **隔離備份環境，避免連帶遭到破壞**：備份環境與正式環境採用各自獨立帳號及網段，並導入多因子驗證，避免共用存取權限（如正式環境的管理員，不應該擁有刪除備份的權限）或長時間維持可寫入連線，確保當正式環境被駭客攻破時，不因帳密共通或通道未斷而連帶遭到破壞。每季至少執行一次實際還原演練，驗證備份能否完整還原。

(3) **建立備援機制，讓關鍵服務不中斷：**由管理階層確認關鍵服務恢復順序、最大可容忍中斷時間（MTPD）及復原點目標（RPO，即容許損失之資料量）；針對關鍵系統備妥備援主機、雲端備援或手動替代作業流程，讓企業受駭後，可迅速復原到最低可行營運狀態（MVO），避免業務徹底停擺。每年至少執行一次重要服務的備援切換演練，確保可在 MTPD 時間內切換運作。

(4) **持續監控，當發現異常能即時處理：**針對員工帳號自非預期 IP 位址登入、備份失敗、備份遭刪除、大量檔案加密等情形，建立明確正常行為基準及相對應的告警規則，避免過多無效訊息產生「告警疲勞」，同時指定負責人員、通報窗口及處置權限，確保異常能即時通知及處理；另外，全面部署端點偵測與回應（EDR）並集中保存重要系統日誌，保存證據資料，確保數位證據保全與事後追查能力。

（三）結語

綜上，因應 AI 帶來的威脅，企業除了應善用政府所提供的資安資源，強化情資掌握、應變能力與防禦實力外，更應回頭確認既有防禦措施是否落實，建議立即從以下 2 個面向著手，強化整體資安防禦與營運韌性：

(1) **縮小攻擊面**：定期盤點資產、關閉不必要的對外服務、及時修補漏洞、落實帳號權限控管，以降低遭受攻擊的風險。
(2) **做好備份備援**：落實 3-2-1 備份原則、定期驗證備份還原及演練備援機制，並持續監控異常活動，確保關鍵業務在遭受攻擊後仍能逐步恢復運作。

對國內企業與機關，資安署亦提供 TWCERT/CC 威脅情資與去識別化的保密協處窗口、《中小企業基本資安防護指引》與《資安事件應變處理行動指引》，以及企業資安諮詢專線 0800-280-280，資安長可轉知轄下單位及委外供應商運用。

參考資料：數位發展部資通安全署，”新型態 AI 攻擊來襲！資安署提出企業防護策略指引呼籲穩紮「資安基本功」”新聞稿，115 年 10 月 21 日。

二、近期資安事件分享

（一）「忘記帳號」功能未落實身分驗證

某機關服務平臺發現遭異常新增 34 組異常帳號，經查主因係為該平臺「忘記帳號」功能身分驗證機制存在漏洞，導致系統誤判憑證驗證狀態，使攻擊者於未完成憑證驗證情況下，仍取得帳號維護權限，並用以新增帳號。該批異常帳號後續雖嘗試存取其他平臺功能，但已被機關既有的權限存取控制機制成功攔阻，故未影響平臺服務正常運作，亦未發現功能

異常或資料遭竄改、外洩等情事，本次事件影響範圍僅限於異常帳號建立，目前機關也已完成漏洞修補作業。

（二）經驗學習（Lessons Learned）

網站登入、帳號申請、密碼重設及權限異動等功能，通常由多個驗證步驟串接而成。除檢驗正常流程之驗證機制有效外，亦須將各類異常情境納入考量，確保系統在驗證失敗、發生例外或無法判斷驗證狀態時，皆能立即中斷後續操作，不會因此跳過檢查或繼續執行後續操作。

OWASP 提出的「安全失敗（Fail Securely）」原則，即強調安全機制發生錯誤或例外時，系統應維持安全狀態，避免因異常而產生安全漏洞：

1. **驗證異常時預設拒絕**：身分驗證、授權或其他安全檢查如失敗、發生例外或無法確認結果，系統應立即停止流程並拒絕操作，不得因未預期的錯誤而略過檢查，貫徹「預設拒絕」原則，防堵因未妥善處理而衍生資安破口。
2. **重要功能應由後端伺服器驗證：**登入、帳號建立、密碼重設及權限異動等重要功能，應由後端伺服器確認必要驗證程序已完成且有效，不得僅依前端所傳入參數或流程狀態決定放行。OWASP 亦強調，核心的身分驗證及授權控制均應在可信任的伺服器端嚴格落實。
3. **異常情況應建立一致處理機制：**對參數缺漏、格式錯誤、驗證服務異常或其他非預期情形，應制訂系統一致且安全的錯誤處理邏輯，確保程式發生各種異常狀態下均能安全地將請求阻絕，以免原有驗證或授權程序失效或被繞過。
4. **將非正常操作納入安全測試：**測試範圍除正常操作功能外，亦應涵蓋參數缺漏或異常、流程參數遭竄改、驗證服務失效及跳過前置步驟等情境。依 OWASP 指引，系統應落實安全失敗原則，將非正常操作與例外處置有效性納入授權驗證測試，避免系統於非正常操作下遭越權繞過。

5. **實施 API 呼叫頻率及流量限制：**應依各 API 的業務特性與敏感層級，設定合理的請求頻率、連線流量或數量限制，並視需要可針對使用者、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，大量蒐集資料而造成機敏資料外洩。對於短時間內暴增的異常查詢行為，應建立自動阻擋或告警機制。

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

三、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 6 萬 8,860 件(減少 2 萬 2,871 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(51%)，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(25%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(9%)，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。

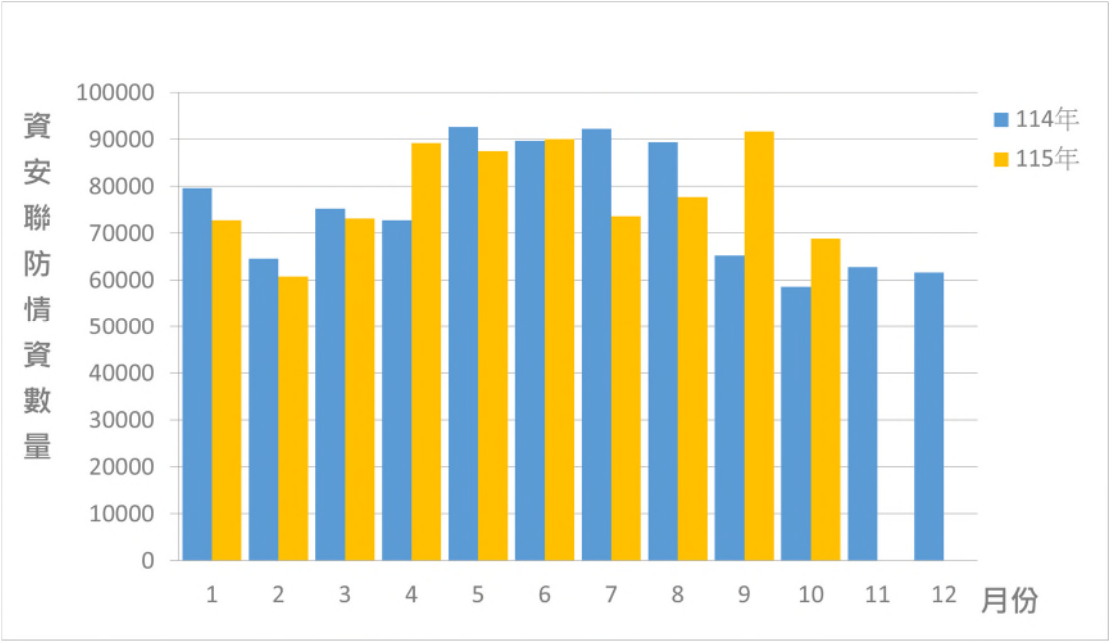


圖 1　資安聯防監控情資統計

2.　本月情資分析：駭客透過釣魚郵件誘騙，竊取帳號憑證

經進一步彙整分析聯防情資資訊，發現近期駭客透過釣魚郵件偽裝 Microsoft SharePoint 文件分享通知，誘騙收件者進入偽造之文件檢視頁面並輸入帳號密碼，以竊取使用者 Microsoft 帳號憑證。此次攻擊並利用合法雲端服務作為釣魚內容載體，以增加釣魚頁面可信度並降低遭資安設備偵測之可能性，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 160 件(包含攻防演練數量 8 件)，為去年同期的 3.02 倍，通報類型以非法入侵為主，占本月通報件數 73.13%。另發現多個機關陸續觸發殭屍網路相關連線，受影響設備多為監視器等聯網設備。近 1 年資安事件通報統計詳見圖 2。

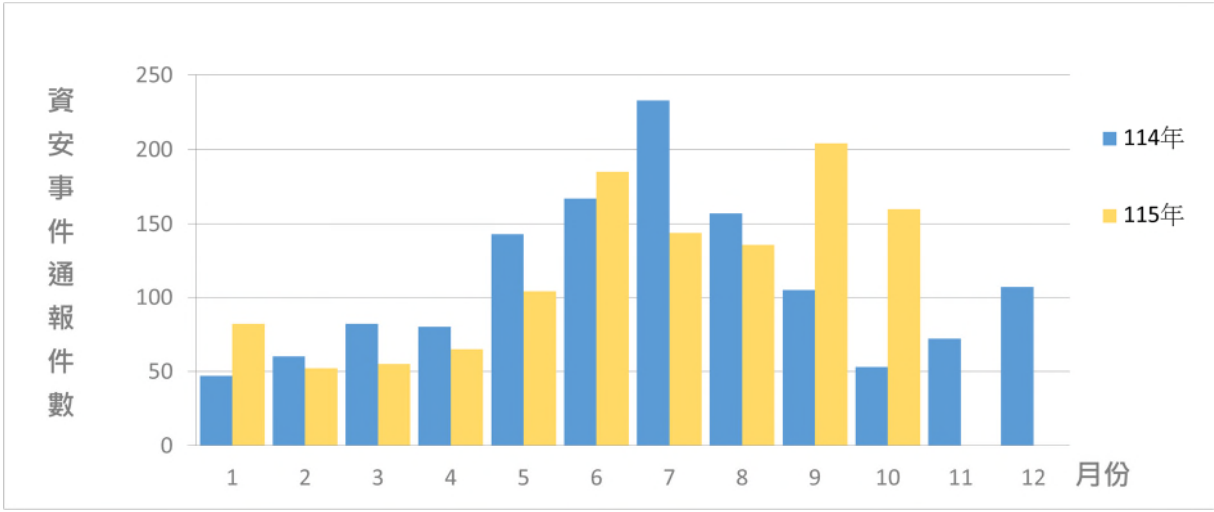


圖 2　資安事件通報統計

四、國際資安新聞

（一）攻擊者利用 CVSS 10.0 的 Bricksforge WordPress 漏洞實現未經身分驗證的遠端程式碼執行(RCE)

（資料來源：The Hacker News**）**

WordPress 資安公司 Patchstack 於 10 月 7 日偵測到針對 WordPress 網站擴充外掛 Bricksforge 漏洞（CVSS 評分為 10.0，CVE-2026-85097）的攻擊行動。該漏洞影響 3.1.8.9（含）以前版本，主要原因是系統在處理表單提交時，對「temporaryFileUploads」參數的 URL 欄位驗證不足，導致未經身分驗證的攻擊者可上傳惡意檔案並在 WordPress 網站上執行任意 PHP 程式碼，進行遠端程式碼執行（RCE）。

分析指出，攻擊者透過不需身分認證的 AJAX 端點請求，取得有效的安全代碼（nonce）以繞過表單的防偽檢查，再利用 GIF/PHP 混合格式（polyglot，將惡意 PHP 程式包裝成圖片）通過檔案類型安全驗證（MIME 檢查），將檔案上傳至暫存目錄，最後再提交特製表單，將帶有惡意 PHP 程式碼的圖片，以.php 為副檔名儲存至正式目錄中，一旦惡意指令被啟動時，攻擊者就能接管網站、存取敏感資料並建立持久存取權

限。建議使用者儘速升級至已修補的 3.1.8.10 或 4.0.1 最新版本，並檢查異常表單提交紀錄及不明 PHP 檔案，以確認網站是否有遭入侵的跡象。

（二）駭客植入可規避掃描的 JavaScript 感染 953 家線上商店，受害者多為 Magento 平臺

（資料來源：The Hacker News）

資安業者 Sansec 揭露一場自 114 年 7 月活躍至今的攻擊行動，累計 953 家線上商店遭駭（其中多數採用 Magento 平臺），攻擊者透過「PolyShell」（CVE-2026-48356，波及約 471 家）與「SessionReaper」（CVE-2025-54236，波及 102 家）漏洞入侵，在網站頁面植入惡意程式碼，利用 Magento CMS 的區塊功能植入惡意 JavaScript 載入程式（尚未確認其究竟是修改既有區塊，或是另行建立新的區塊），當使用者瀏覽遭入侵的網站時，瀏覽器便會向攻擊者控制的外部伺服器請求後續指令。該程式碼甚至進一步藉由瀏覽器指紋檢查排除自動化掃描，讓資安掃瞄工具無法偵測，也確保只有正常訪客會接收到惡意酬載（payload）。由於攻擊者最終的具體攻擊意圖仍不明朗，專家建議網站管理者應全面清查 Magento CMS 是否存在可疑帳號、儘速套用安全性更新，並執行強密碼。

參考附錄-本月重要漏洞警訊

（一）漏洞警訊

類別	內容說明
資安監控平臺 Splunk Enterprise **嚴重程度：** (CVE-2026-76268：CVSS v3.1 9.8)	● Splunk Enterprise 的 Search Head 叢集存在遠端程式碼執行漏洞(CVE-2026-76268)。 ● 未經身分鑑別之攻擊者若可存取叢集成員的 Patroni REST API，可變更關鍵設定，進而於主機執行作業系統指令。 ● 官方已釋出修補版本，建議將受影響的 10.4 或 10.2 分支分別更新至 10.4.3 或 10.2.7(含)以上版本，並限制 Patroni REST API 的網路存取。
備份與復原軟體 Veeam Backup & Replication **嚴重程度：** (CVE-2025-64393：CVSS v4.0 9.4)	● Veeam Backup & Replication 存在不安全反序列化漏洞(CVE-2025-64393)，原廠於本年 10 月公告修補。 ● 具有 Backup Viewer 低權限角色的攻擊者，可利用 Mount Service 於備份伺服器執行任意程式碼。版本 13 不受此漏洞影響。 ● 官方已釋出修補版本，建議將受影響的版本 12 更新至 12.3.2 P4(build 12.3.2.4934)或原廠公告之後續修補版本，並檢視備份管理帳號權限。
應用交付與遠端存取設備 Citrix NetScaler ADC / Gateway **嚴重程度：** (CVE-2026-107406：CVSS v4.0 9.5)	● Citrix NetScaler ADC 與 Gateway 存在記憶體溢位漏洞(CVE-2026-107406)。 ● 在使用 SAML 驗證且符合公告版本及設定條件時，未經身分鑑別之遠端攻擊者可觸發記憶體溢位，造成任意程式碼執行或阻斷服務；受影響的 SAML SP / IdP 角色依版本而異。 ● 官方已釋出修補版本，一般分支建議更新至 14.1-73.46 或 13.1-64.29(含)以上；FIPS / NDcPP 分支請依公告對照表更新，勿混用一般分支版本。

（二）已知遭駭客利用之漏洞

類別	內容說明
程式碼與開發管理平臺 GitLab CE / EE **嚴重程度：** (CVE-2026-97229：CVSS v3.1 10.0) (CVE-2026-110264：CVSS v3.1 10.0)	● GitLab CE / EE 存在正規表示式處理之整數溢位漏洞(CVE-2026-97229、CVE-2026-110264)。CISA 已於 10 月 29 日將前者列入 KEV 清單。 ● 未經身分鑑別之攻擊者在特定條件下，可透過特製正規表示式的處理程序，於 GitLab 伺服器執行任意程式碼。兩項漏洞須分別確認修補狀態。 ● 官方已釋出修補版本，建議依使用分支更新至 19.5.1、19.4.3、19.3.6 或公告所列其他修補版本(含)以上。自行編譯或使用非官方映像者，亦須依公告更新 Ruby。
電子郵件安全設備 Cisco Secure Email Gateway **嚴重程度：** (CVE-2026-76519：CVSS v3.1 9.8)	● Cisco Secure Email Gateway 存在任意檔案寫入漏洞(CVE-2026-76519)。CISA 已於 10 月 14 日列入 KEV，Cisco 亦確認已有實際利用情形。 ● 當 AMP File Reputation 已啟用並套用至郵件政策，且掃描元件為受影響版本時，未經身分鑑別之攻擊者可寄送惡意附件，進而以 root 權限執行指令。 ● 官方已釋出修補，請確認 Content Scanner Tools 已更新至 25.3.0.5525(含)以上；亦可依公告升級 AsyncOS 至 15.5.5-014 或 16.5.0-780 等修補版本，並檢查入侵跡象。
電子郵件安全設備 Fortinet FortiMail **嚴重程度：** (CVE-2026-104286：CVSS v3.1 9.8)	● Fortinet FortiMail 存在路徑遍歷與 NULL 字元處理不當漏洞(CVE-2026-104286)。CISA 已於 10 月 1 日列入 KEV，Fortinet 亦通報已有實際利用情形。 ● 未經身分鑑別之遠端攻擊者可傳送特製 HTTP / HTTPS 請求，在底層系統寫入任意檔案，造成重大系統安全風險。 ● 官方已釋出修補版本，建議依分支更新至 8.0.2、7.6.7 或 7.4.9(含)以上；其他分支依公告處置。尚未完成修補時，可先依公告停用 IBE 功能或限制 Webmail 存取。

類別	內容說明
網站程式執行環境 PHP **嚴重程度：** (CVE-2026-109618：CVSS v3.1 9.8) (CVE-2026-109619：CVSS v3.1 8.1)	● PHP 存在記憶體處理漏洞(CVE-2026-109618、CVE-2026-109619)。CISA 已於 10 月 28 日將兩項漏洞列入 KEV 清單。 ● 未經身分鑑別之攻擊者可透過特製 multipart/form-data 請求，在特定記憶體與請求處理條件下，於伺服器執行任意程式碼；應盤點網站及內嵌 PHP 的應用系統。 ● 官方已釋出修補版本，建議依分支更新至 8.5.12、8.4.27、8.3.36 或 8.2.35(含)以上；Windows 套件請採用含 Brotli 修補的-1 重建版，並依公告確認 Session 設定與停止支援版本的處置。
伺服器執行環境與壓縮元件 Node.js / Brotli **嚴重程度：** (CVE-2026-111497：CVSS v3.1 9.8)	● Node.js 所使用的 Brotli 解壓縮元件存在越界寫入漏洞(CVE-2026-111497)。CISA 已於 10 月 27 日將此 Brotli 漏洞列入 KEV 清單。 ● 應用程式若透過 node:zlib 解壓縮不受信任的 Brotli 資料，攻擊者可能以特製資料觸發記憶體毀損，造成服務中斷、資訊洩漏或遠端程式碼執行。 ● 官方已釋出安全更新，建議將 Node.js22、24、26 分支分別更新至 22.23.4、24.22.1、26.12.1(含)以上，並重新部署使用受影響元件的服務與映像。
防火牆與集中管理設備 Palo Alto Networks PAN-OS **嚴重程度：** (CVE-2026-0322：CVSS v4.0 8.6)	● PAN-OS 存在程式碼注入漏洞(CVE-2026-0322)。CISA 已於 10 月 14 日列入 KEV，Palo Alto Networks 亦確認觀察到少量實際利用。 ● 經過驗證的攻擊者可透過網路存取防火牆，並以 root 權限執行任意程式碼。Prisma Access 與 Cloud NGFW 不受此漏洞影響。 ● 官方已釋出修補，請依 PAN-OS 分支對照公告更新，例如 12.2.4、12.1.10-h2、11.2.16 或其他適用修補版本；並將管理介面限制於受信任的內部來源。

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。