資通安全網路月報

一、資安長話短說

因應前沿 AI 漏洞暴增，資安長的處置策略與應對建議

(一)預測 CVE 數量遽增至 6.6 萬個

國際資安應變組織（Forum of Incident Response and Security Teams, FIRST）於 2026 年 6 月 15 日第 38 屆年會發布年中漏洞預測報告，將 2026 年「常見漏洞與暴露」（Common Vulnerabilities and Exposures, CVE）總量預估由 5 萬 9,427 個增加至約 6 萬 6,000 個[註 1]。

FIRST 分析，這波 CVE 數量暴增，因素包含有 AI 輔助漏洞挖掘，以及 VulnCheck 等「最後手段 CVE 編號機構（CNA-of-Last-Resort）核發量年增 3,119%[註 2]。

(二)CVE 揭露量暴增，可利用比例未同步上升

FIRST 報告提醒，漏洞總量上升，實際遭利用或具高利用可能的漏洞比例並未跟著增加。以美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）公布「已知遭利用漏洞（Known Exploited Vulnerabilities, KEV）目錄」與 EPSS（Exploit Prediction Scoring System）分數高於 10%作為門檻過濾，2026 年揭露的 CVE 僅約 7%具備實

際可利用性；截至 5 月 1 日，KEV 清單累計 1,587 筆。

(三)修補量能成為新的瓶頸

Anthropic 於 5 月 22 日發布的 Project Glasswing 計畫進度報告揭露一個現實，在已對外揭露的 530 個重大漏洞中，僅 75 個完成修補，其中 65 個發布公告，平均一個重大漏洞需要約兩週開發修補[註 3]。挖掘漏洞的速度已遠超過修補漏洞的速度，瓶頸從「找到」移向「修好」。2026 年 4 月號資通安全網路月報（下稱本刊）曾說明漏洞從揭露到武裝化的中位數時間已縮短至數小時，對照本月數據，各機關面臨的是待修清單變長、可反應時間變短的雙重壓力。被動等待廠商釋出修補再行動的模式，在 2026 下半年將難以為繼。

(四)給資安長的處置策略

綜合 FIRST 對全球資安團隊的建議，並延續本刊四月號「策略」、「管理」及「技術」三面向的架構，建議各機關資安長採取下列行動：

1. 以風險導向建立漏洞修補機制

運用 KEV 等指標進行漏洞風險分級，以實際可利用性作為修補優先順序，優先處理高風險及對外服務系統漏洞。

2. 預為準備漏洞修補量能

漏洞修補工作量在 2026 下半年可能倍增，漏洞修補應擴大測試與部署的自動化程度，並建議於委外契約中明定廠商的漏洞修補時限之服

務水準協議（Service Level Agreement, SLA）。

3. 導入防禦性 AI 工具

攻擊方已規模化使用 AI 來攻擊，防禦方若仍以人工模式處理漏洞，雙方時間差距將持續擴大，故機關應評估以 AI 輔助漏洞掃描、情資分析與修補驗證，並以「平均修補時間」（Mean Time To Remediate, MTTR）作為衡量成效的核心指標。

在今年 7 月所召開的國家資通安全會報第 1 次委員會議中，行政院鄭副院長明確指示，為因應前沿 AI 模型能迅速偵測漏洞並發動攻擊的威脅，應同步導入 AI 技術深化防禦。此外，數位發展部後續將公布漏洞管理指引，屆時各機關須以最快速度依循指引進行修補，或採取相應的防護措施。面對全年漏洞恐增加至 6.6 萬的預測趨勢，各機關無須過度恐慌，但必須調整防護思維，將有限的人力精準聚焦於易遭利用的關鍵漏洞，並以「加速處置與復原」為核心努力目標。

註 1：https://www.first.org/newsroom/releases/20260615
註 2：https://www.first.org/blog/20260615-vulnerability-forecast-update
註 3：https://www.anthropic.com/research/glasswing-initial-update

二、近期政策重點

(一)第二屆「產品資安漏洞獵捕活動」自 7 月 1 日起於臺灣電腦網路危機處理暨協調中心（Taiwan Computer Emergency Response Team/Coordination

Center, TWCERT/CC）官網開放軟體廠商（藍隊）報名，並於 9 月 1 日起受理紅隊國內白帽駭客菁英報名，相關活動預計於 10 月 1 日正式登場，活動為期 2 個月。

(二)為協助各機關強化公務出國人員資通訊設備管理，防止公務機密資料遭竊取、竄改、毀損、滅失或洩漏，爰資安署擬訂定「公務出國（含大陸地區、香港及澳門）資通訊設備管理須知」，已於 7 月 1 日頒布施行。

(三)衡酌資訊技術日新月異、設備類型繁雜，《資通安全管理法》第 11 條第 1 項及第 27 條第 1 項所述「自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時，亦同」之具體內涵與適用邊界，允宜進一步闡明，爰資安署業於 6 月 29 日函頒上開條文之解釋令，特就「傳播設備」、「網際網路接取服務」及「於維護資通安全必要時」等名詞及範圍予以明確定義，以利各機關據以判別及執行。

三、近期資安事件分享

AI 智能客服提示詞注入風險及改善措施

近期發現機關網站提供 AI 智能客服，遭檢測確認存在可利用「提示詞注入（Prompt Injection）」，對其要求執行超出設計範圍的任務，例如要求讀取/etc/passwd 及/etc/shadow 等檔案，導致敏感資料洩漏疑慮。後續機關已

限制該程式存取權限，並建立對話過濾機制，避免 AI 智能客服遭有心人士利用。

經驗學習(Lessons Learned)

提示詞注入係攻擊者透過一般提問或對話方式，讓 AI 功能依其設計的內容進行回應，甚至執行非預期操作，這類手法不一定需要懂程式語言，也不一定要撰寫複雜程式。除直接輸入之文字，文件、網頁或其他外部資料亦可能成為利用來源，也因其形式接近一般文字互動，較不易於第一時間辨識。其風險包含回應內容遭操控與未妥善限制系統資源存取權限，建議各機關於導入 AI 客服或聊天機器人時，宜特別留意下列事項：

1. 權限最小化與系統資源、資料範圍限制：應限制 AI 功能僅存取經核准之資料範圍，並以白名單方式提供可介接之業務應用程式介面（Application Programming Interface, API）；後端服務帳號則應依最小權限原則設定，僅允許存取完成業務所需之特定資料表、欄位及功能。
2. 建立輸入內容與外部資料之過濾機制：應針對對話框輸入及文件、網頁、郵件、附件等外部資料建立過濾與風險判斷機制，並對涉及系統路徑、系統指令、敏感資訊查詢或意圖改寫既有規則之內容設置阻擋、過濾或告警，以降低提示詞注入風險。
3. 強化系統提示詞（System Prompt）防護：開發時應於系統底層的「系統提示詞」中，明確設定 AI 之角色定位、回應範圍及不可執行事項，例如

限制其僅能提供便民客服資訊，不得執行系統指令、讀取伺服器檔案或變更角色設定。透過預先設定明確之行為邊界，可降低 AI 受惡意提示詞影響而偏離原有功能之風險。另應持續監控其輸入內容、模型回應、外部資料讀取及系統資源存取情形，以利即時發現異常行為。

四、資通安全趨勢

(一) 我國政府整體資安威脅趨勢

事前聯防監控

本月蒐整政府機關資安聯防情資共 9 萬 0,114 件(較上月增加 2,603 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(23%)，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。

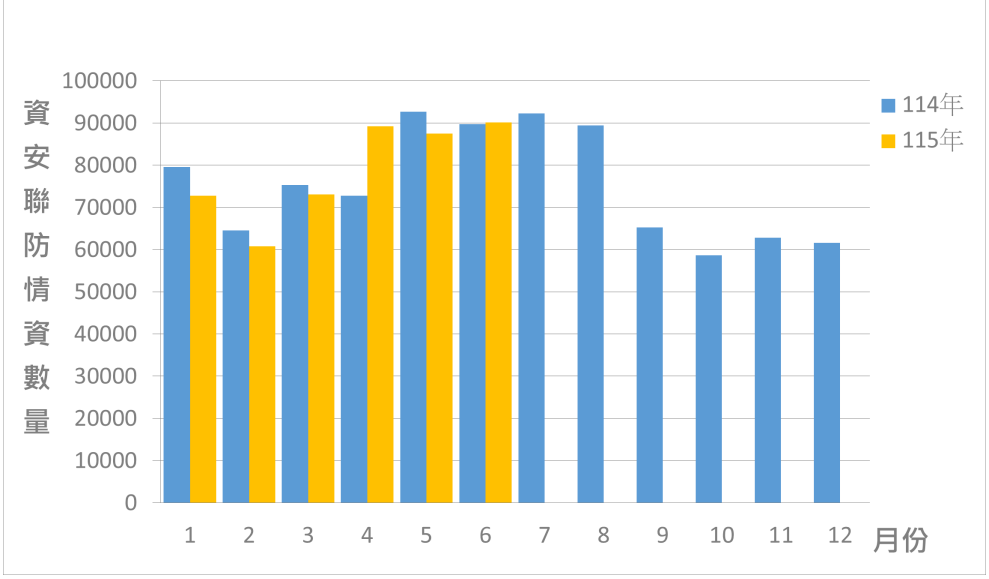

圖 1 資安聯防監控資安監控情資統計

駭客濫用免費圖片分享空間作為惡意檔案散布平台

經進一步彙整分析聯防情資資訊，發現近期駭客濫用 Cloudflare R2 作為惡意程式下載站，Cloudflare R2 是 Cloudflare 所提供的物件儲存（Object Storage）服務，可讓使用者透過網際網路儲存與提供各種檔案，例如圖片、影片、備份資料、軟體安裝檔及網站內容。惟駭客利用此服務散布惡意程式，以規避資安偵測機制，進而達成植入惡意程式之目的，相關情資已提供各機關聯防監控防護建議。

事中通報應變

本月資安事件通報數量共 187 件(包含攻防演練數量 104 件)，為去年同期的 1.12 倍，通報類型以非法入侵為主，占本月通報件數 62.50%。本月攻防演練發現，部分機關網站存在未經登入或權限驗證即可透過連結下載檔案，或目錄列表(Index of)功能未妥善關閉等情形，致外部可檢視目錄結構及其中檔案內容；另有委外建置網站因後台預設帳號密碼具規律性，遭猜測登入利用。近 1 年資安事件通報統計詳見圖 2。

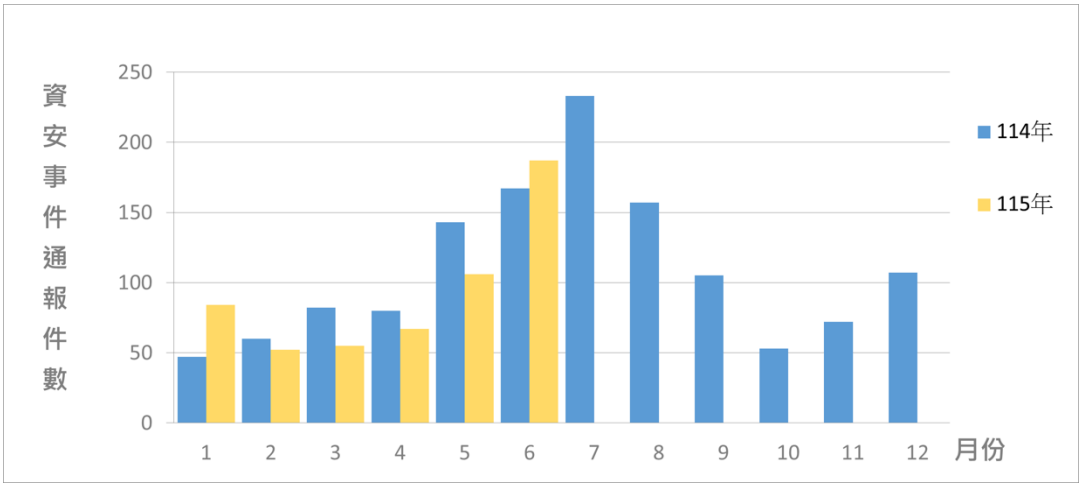

圖 2 資安事件通報統計

(二) 重要漏洞資訊，詳請參考附錄。

五、國際資安新聞

美國 CISA 修訂聯邦漏洞修補要求，以應對 AI 威脅時代

(資料來源：Dark Reading)

美國網路安全暨基礎設施安全局（CISA）於新版約束性操作指令（Binding Operational Directive, BOD）26-04 中，採用風險矩陣機制修訂聯邦漏洞修補要求，規定聯邦機構須於 3 日內修補高風險漏洞，並允許依風險評估結果延後處理低風險漏洞。新指令取代既有兩項聯邦漏洞修補規範（BOD 19-02 及 BOD 22-01），反映 AI 技術發展下，漏洞修補與威脅應處日益複雜的挑戰。該指令建立分級修補機制，綜合考量已知遭利用漏洞（KEV）、資產是否對外公開、攻擊者是否可透過自動化方式利用漏洞，以及漏洞遭利用後是否可取得部分或完整系統控制權等因素，作為漏洞修補優先順序的依據。此外，各機關須進行數位鑑識分類（Forensic Triage），確認受影響資產是否已遭入侵，並應於 60 日內完成漏洞管理流程更新，於 180 日內全面落實相關措施，以確保漏洞能依規定時限完成修補。

美國聯邦通訊委員會（FCC）通過緊急警報系統與海底電纜新資安規則

(資料來源：Cyber Scoop)

美國聯邦通訊委員會（FCC）通過新的網路安全規則，強化緊急警報系

統（EAS）及無線緊急警報（WEA）的資安防護，並同步更新海底電纜供應商的安全管理規範。新規則要求相關單位於存取及更新警報系統時，須採行強密碼、即時套用安全修補及部署防火牆等資安防護措施。此外，FCC 建立新的警報身分驗證機制，以驗證警報來源並防止未經授權或重複發送訊息。針對海底電纜，FCC 修訂監管規定，符合高安全標準並完成自我認證的供應商，可免除國家安全許可審查，亦擴大對海底電纜關鍵營運功能的監管權限，以強化關鍵基礎設施的資安韌性。

六、資安宣導資訊

駭客以研討會偽冒 QR Code 釣魚騙取個資

QR Code 為生活帶來極大便利性，卻也潛藏著被惡意利用的風險！近期發生真實案例，駭客利用公開研討會活動海報的官方報名 QR Code，將其竄改成惡意版本後進行散布，民眾掃碼後誤入釣魚網頁填寫報名資料，導致個人隱私外洩。

這種網路攻擊又稱為「Quishing（QR Code 網路釣魚）」，是將釣魚網址藏在條碼圖片中，民眾必須提高警覺避免受駭。

1. 常見情境：

(1) 竄改覆蓋：會議海報、停車繳費機或共享單車，被惡意貼紙覆蓋，或經竄改真實 QR Code 後重新印製散布張貼於公共場域。

(2) 偽造通知：假冒訂單異常、退稅、罰單，或偽裝 IT 部門寄發「帳

號重新驗證」信件。

2. 防護措施：「掃碼停看聽」

(1) 「停」摸一摸、看一看：掃描實體條碼前，先觀察或觸摸邊緣，檢查是否有材質不同或被異常「貼紙」覆蓋的痕跡。

(2) 「看」先看網址再操作：使用掃描後會浮現「網址預覽」的 App（現行 Android、iOS 手機預設相機多已具備），請勿秒點！先仔細核對網域拼字是否正確(如將 microsoft 拼錯成 micros0ft)，若遇到隨機亂碼或短網址務必提高警覺。

(3) 「聽」提高警覺多求證：遇到「優惠、停權、繳費」等話術，要求輸入信用卡號碼、個人資料或下載 App，請透過官方管道查證。

掃描前多停一秒、多看一眼、多問一句，就能避開陷阱，安心保護荷包與個資！

七、近期重要資安會議

(一) 公私協力雙軌齊下，強化中小企業資安防護力

為落實「資安防護，政府相挺」政策方向，數位發展部資通安全署為提升中小企業整體資安防護能量，今（2026）年開辦資安培訓課程與資安專家諮詢服務，協助企業降低營運安全風險，轉化資安力為競爭力，辦理項目如下：

1. 2 梯次免費資安培訓課程「防駭與資料保護基礎必修課」：每梯次

為期 2 天，邀請具實務經驗的資安專家授課，並由指標性企業進行經驗分享，以深入淺出的方式引導企業逐步建構資安防護能力。培訓課程第一梯次已辦畢，第二梯次將於 7 月 17 日至 18 日登場，將同步辦理實體課程及線上直播，方便全臺各地中小企業參加。

2. 100 場以上免費、一對一「資安專家會客室」諮詢服務：針對防範駭客入侵、保護業務機敏資料等關鍵營運議題，提供防護行動建議，協助企業建立有效資安策略與管理措施，降低營運安全風險，服務開放期間自 6 月 11 日起至 10 月底，每週開放 2 日，每日提供 3 場次。諮商後 2 週內提供客製化的具體行動建議，並將主動關懷企業辦況，協助中小企業強健資安防護體質。

(二) 資安主管研習會議

於 7 月 16 日辦理資安主管研習會議，邀集對象為資安責任等級 A 級之政府各級機關(構)及特定非公務機關、資安責任等級 B 級之政府各級機關(構)，另今年更擴大邀請總統府、國家安全會議及立法院、司法院、考試院、監察院與特定非公務機關的資（訊）安主管共同參與，期盼藉此建構更縝密的資安聯防體系，以實際行動表達對國家資安聯防與交流機制的堅定支持。

參考附錄-重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	網頁伺服器 F5 NGINX Open Source、NGINX Plus、NGINX Gateway Fabric 嚴重程度： (CVE-2026-42530：CVSS 8.1) (CVE-2026-42055：CVSS 8.1)	● 研究人員發現 NGINX 的 HTTP/3 模組（ngx_http_v3_module）存在釋放後使用漏洞（CVE-2026-42530），Proxy 與 gRPC 模組存在堆積緩衝區溢位漏洞（CVE-2026-42055）。 ● 於特定非預設組態下，未經身分鑑別之遠端攻擊者可觸發記憶體毀損造成服務中斷（DoS），並可能於 ASLR 停用或被繞過時執行任意程式碼。 ● 官方已發布公告（K000161614），建議依受影響版本儘速完成更新或套用緩解措施。
	行動裝置閘道設備 Ivanti Sentry 嚴重程度： (CVE-2026-10520：CVSS 10.0) (CVE-2026-10523：CVSS 9.8)	● 研究人員發現 Ivanti Sentry 存在作業系統命令注入與身分鑑別繞過漏洞(CVE-2026-10520、CVE-2026-10523)。 ● 未經身分鑑別之遠端攻擊者可分別以 root 權限執行任意程式碼，或建立任意管理員帳號並取得完整管理權限。 ● 官方已釋出修補版本，建議儘速更新至 Ivanti Sentry 10.5.2、10.6.2 或 10.7.1(含)以上版本。
	VPN 與網路安全設備 Check Point Security Gateways 與 Spark Firewalls 嚴重程度： (CVE-2026-50751：CVSS 9.3)	● 研究人員發現 Check Point Security Gateways 與 Spark Firewalls 存在 IKEv1 憑證驗證邏輯缺陷(CVE-2026-50751)。 ● 未經身分鑑別之遠端攻擊者可繞過使用者驗證，無須透過有效使用者密碼之情形下建立遠端存取 VPN 連線，進而存取內部資源；另官方已觀察到實際利用情形。 ● 官方已提供修補與暫時緩解措施，建議依受影響版本儘速完成更新與設定調整。
已知遭駭客利用之	網路設備管理平台 Ubiquiti UniFi OS	● CISA 已於 6 月 23 日將 CVE-2026-34908、CVE-2026-34909 與 CVE-2026-34910 列入

警訊	類別	內容說明
漏洞	（Cloud Gateway、Dream Machine、UniFi OS Server 等） 嚴重程度： (CVE-2026-34908：CVSS 10.0) (CVE-2026-34909：CVSS 10.0) (CVE-2026-34910：CVSS 10.0)	KEV 清單；資安業者已觀察到攻擊者串聯利用此三項漏洞散布惡意程式並建立未授權管理者帳號。 ● 三項漏洞可串聯利用：前兩者為驗證閘道繞過（不當存取控制與路徑穿越），後者為套件更新功能之命令注入，未經身分鑑別之遠端攻擊者可取得 root 權限並完全控制設備。 ● 官方已釋出修補版本，建議儘速更新並避免將管理介面暴露於外部網路。
	網路管理系統 Cisco Catalyst SD-WAN Manager 嚴重程度： (CVE-2026-20262：CVSS 6.5)	● CISA 已於 6 月 15 日將 CVE-2026-20262 列入 KEV 清單，Cisco 證實該漏洞已遭限定範圍之零時差攻擊利用。 ● 此漏洞因檔案上傳未正確驗證輸入（路徑穿越），已通過身分鑑別之遠端攻擊者可於系統任意位置建立或覆寫檔案，進而提權至 root。 ● 官方已釋出修補版本，請依公告儘速更新（無替代緩解措施）。
	網頁瀏覽器 Google Chrome（Chromium V8） 嚴重程度： (CVE-2026-11645：CVSS 8.8)	● CISA 已於 6 月 9 日將 CVE-2026-11645 列入 KEV 清單；此為 2026 年第 5 個遭實際利用之 Chrome 零時差漏洞。 ● 此漏洞為 V8JavaScript 引擎之越界讀寫，遠端攻擊者可透過特製 HTML 網頁觸發堆積記憶體毀損，於沙箱內執行任意程式碼。 ● 官方已釋出修補版本，建議將 Chrome／Chromium 核心瀏覽器更新至最新版本。

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