資通安全網路月報

一、資安長話短說

（一）「先竊取、後解密」，讓機密資訊已暴露於量子風險

後量子密碼（Post-Quantum Cryptography，PQC）遷移期限聽起來很遙遠，但想像一下，您今天在網路上傳送的金融交易、個人敏感或企業機密資訊，雖然透過現有加密技術保護，但駭客極有可能正偷偷將這些資料攔截並儲存起來，等待未來大型量子電腦技術成熟後，瞬間破解這些加密內容。這種被稱為「先竊取、後解密」（harvest now, decrypt later）的攻擊模式，已逐漸成為現實世界中的重大資安威脅。

量子計算專家 Michele Mosca 提出了一個簡單的公式，「機敏資訊保密的年限（X）」加上「系統升級到後量子加密所需的時間（Y）」，這兩個時間加起來，如果比「大規模通用量子電腦所需的時間（Z）」還要長（即 X + Y > Z ），代表您的機密資訊在還沒超出保密期限前就可能被量子電腦破解，根據過去經驗，全面更換特定類型密碼系統恐曠日費時，所以最好及早規劃以應對即將來襲的量子風險。

（二） 觀測國際動態：解析美國後量子政策

美國於 2026 年 6 月 22 日發布「保護國家免受先進密碼學攻擊」（Securing the Nation Against Advanced Cryptographic Attacks）[註 1] 行政命令，將聯邦資訊系統過渡至 PQC，並協助關鍵基礎設施提供者完成其遷移，以維護國家安全。該行政命令主要圍繞在「統籌政策規劃、技術引導協助、修訂採購法規」，並提出以下多項限期具體行動：

1. **確立負責人與發布指引要求盤點高價值資產（30 天、90 天內）：**
   各機關應於 30 天內確立「PQC 遷移負責人」；白宮管理與預算辦公室（Office of Management and Budget，OMB）應於 90 天內發布指引，要求各機關盤點其高價值資產（High Value Asset，HVA）與高影響系統（High Impact Systems）清單（不含國家安全系統）[註 2、3]，制定並提交相關執行計畫。
2. **啟動 PQC 遷移試辦計畫與加速驗證流程（180 天內）：**
   美國國家標準與技術研究院（National Institute of Standards and Technology，NIST）應針對其所屬或營運的特定資訊系統，啟動 PQC 遷移試辦計畫，並預計於 2027 年底前完成。商務部則應修訂「密碼模組驗證計畫（Cryptographic Module Validation Program，CMVP）」所採用之流程，以加速密碼模組驗證作業。
3. **發布密碼物料清單基本要素指引（270 天內）：**國土安全部應發布公開

指引，明定「密碼物料清單(Cryptographic Bill of Materials，CBOM)」應具備之基本要素，並確保未來能以自動化方式評估軟硬體組件所使用之密碼資產。

4. **修訂採購規範與強化漏洞揭露要求 （180 天、270 天內）：**聯邦採購法規委員會應於 180 天內發布《聯邦採購法規》(Federal Acquisition Regulation，FAR) 草案，強制要求受規範的承包商 (covered contractors) 於 2030 年 12 月 31 日前遵守 PQC 演算法標準。另應於 270 天內修訂《漏洞揭露計畫》規則草案，確保承包商落實 NIST 指引之漏洞揭露政策 (Vulnerability Disclosure Policies，VDPs)，包含揭露加密機制缺失，以及是否使用未經 FIPS 核准之演算法。
5. **明確訂定遷移時限 (中長期目標)：**要求各機關所有 HVA 及高影響系統，全面遷移並採用 PQC 技術，應於 2030 年 12 月 31 日前進行「金鑰建立 (Key establishment)」，且於 2031 年 12 月 31 日前進行「數位簽章 (Digital signatures)」。
6. **協助關鍵基礎設施提供者制定 PQC 遷移計畫：**各關鍵基礎設施領域主管機關 (Sector Risk Management Agency，SRMA) [註4]，應與國土安全部合作，協助關鍵基礎設施所有者和營運者制定 PQC 遷移計畫。

（三） 我國政府機關政策規劃：

從以上美國最新公布的行政命令可以發現，面對量子電腦「先竊取、

後解密」風險，美國採取透過限期具體措施，加速聯邦機關及相關供應鏈逐步落實 PQC 遷移。而我國亦已及早布局，例如數位發展部數位產業署協同「後量子資安產業聯盟」於 2025 年發布《後量子密碼遷移指引》，結合產官學界共同推動資安產業後量子資安技術研發與應用落地。

此外，數位發展部資通安全署已規劃於今年年底前發布我國《政府機關後量子密碼遷移政策》，引導政府機關整體遷移期程，並同步美國、歐盟等國際規範以及持續關注國際趨勢變動與最新技術發展情形，擬訂《後量子密碼遷移實務參考手冊》，以提供各機關執行遷移作業時之參考依循路徑及過渡期補強機制。

（四） 給資安長的建議

美國最新政策動向顯示 PQC 遷移並非是未來議題，而是攸關資安的現在進行式，為順利引導機關穩健推動 PQC 遷移作業，並銜接未來我國 PQC 遷移政策的落實執行，建議資安長現階段可借鏡美方策略，主動採取以下 3 項事先準備作為：

1. **盤點機敏資訊與密碼資產：**全面盤點各機敏資料「保密期限」，並藉由資料的產製、傳輸與儲存路徑，對應其資料流程相關之資訊系統、設備、軟體、憑證、公開金鑰基礎建設（Public Key Infrastructure，PKI）、網路通訊協定及第三方服務，識別其中使用的加密演算法以建立密碼資產清冊，及排列後續 PQC 遷移的優先順序。

2. **系統導入密碼敏捷性：**系統設計開發階段建議導入「密碼敏捷性（Crypto-agility）」的模組化設計，確保未來進行加密機制變更時具備靈活調整加密演算法的彈性，以利未來進行 PQC 遷移作業。
3. **委外契約條款增訂漏洞揭露要求：**在系統未具抵禦量子攻擊能力前，建議委外契約中增訂要求系統委外廠商主動揭露加密機制缺失，以識別具量子脆弱性的演算法。

面對「先竊取、後解密」的量子威脅，世界各國資安防禦體系正迎來一場前所未有的全新挑戰，但同時也是我國構築「數位信任」與可信賴供應鏈的轉型機會，然而 PQC 遷移是一場跨技術、業務流程與組織治理的系統性工程，唯有及早規劃並逐步落實遷移，才能確保在量子防衛戰中贏得先機。

註 1：The White House. （2026, June 22）. *Securing the nation against advanced cryptographic attacks*. https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/

註 2：「高價值資產」（High Value Asset，HVA）係指依據 OMB 備忘錄 M-19-03《透過強化高價值資產計畫以提升聯邦機關資通安全》或任何後續文件指定為高價值資產之聯邦資訊或系統。

註 3：「高影響系統」係指在機密性、完整性或可用性等安全目標中，至少有一項被評定為《聯邦資訊與資訊系統安全分類標準》（FIPS 199）「高」潛在影響值之資訊系統。

註 4：各關鍵基礎設施領域主管機關為 2024 年 4 月 30 日《國家安全備忘錄第 22 號：關鍵基礎設施安全與韌性》（或其後續文件）所定義。

二、近期政策重點

發布《資安事件應變處理行動指引》，協助企業應對資安威脅：

數位發展部資通安全署於 7 月 31 日發布《資安事件應變處理行動指引》，內容包含準備、偵測與應變處理、通報與外部溝通、復原與持續改善等 4 大核心階段及檢核清單，並提供設備感染、帳號被盜、網路釣魚、商業支付詐欺、勒索軟體及 DDoS 等 6 大常見情境之標準處理流程，協助企業非技術人員採取損害控制措施，降低財務與營運衝擊。

三、近期資安事件分享

網站驗證機制失效 爆發嚴重資安事件

近期發現機關網站密碼重設與一次性密碼驗證機制失效事件，攻擊者成功繞過「雙重驗證」修改密碼，如網站提供以電子郵件驗證碼重設密碼功能，惟驗證碼以明碼方式存在於網頁原始碼，攻擊者查得使用者電子郵件後，無須實際收取郵件，即可取得驗證碼並修改密碼。此外，攻擊者查得網站管理員電子郵件後，透過攔截網站請求封包發現密碼重設路徑，並在未完成身分驗證的情況下，可直接進入該頁面修改密碼；攻擊者在使用新密碼登入後，網站未將一次性密碼透過其他管道傳送給合法使用者，而直接將該密碼回

傳至瀏覽器，攻擊者藉由封包內容取得該密碼並繞過第二階段驗證，成功登入管理帳號，詳見圖 1。

圖 1 驗證機制失效示意圖

經驗學習（Lessons Learned）

網站雖設有電子郵件驗證碼、密碼重設及一次性密碼等安全機制，惟驗證資訊暴露於前端，或後端未確認重設流程及使用者身分，仍可能使各項驗證措施遭逐一繞過，建議從下列面向進行強化：

(一) **強化密碼重設流程驗證**：重設 Token 或驗證碼應採安全隨機方式產生，並具備「限時、單次、綁定原帳號」三大特性，即限定用於原申請帳號及該次密碼重設作業，設定有效期限及單次使用限制。伺服器確認憑證有效後，始得允許修改密碼，避免僅憑重設頁面網址即可操

作。

(二) **避免驗證資訊暴露於前端**：電子郵件驗證碼及一次性密碼不得出現在網頁原始碼、隱藏欄位或伺服器回傳內容中。前端僅負責接收使用者輸入，憑證保存及驗證應由伺服器或可信任的身分驗證服務執行；完成一次性密碼驗證前，不得授予完整登入權限。

(三) **重設密碼後終止既有存取權限**：密碼重設完成後，應立即使重設憑證失效，終止原有登入工作階段，並要求使用者依正常登入流程重新驗證密碼及一次性密碼，不宜直接建立登入狀態，避免密碼重設功能成為繞過登入驗證的途徑；另應通知帳號持有人，以利及早發現非本人操作。

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) 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 7 萬 3,650 件(減少 1 萬 6,464 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類 (54%)，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（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 2。

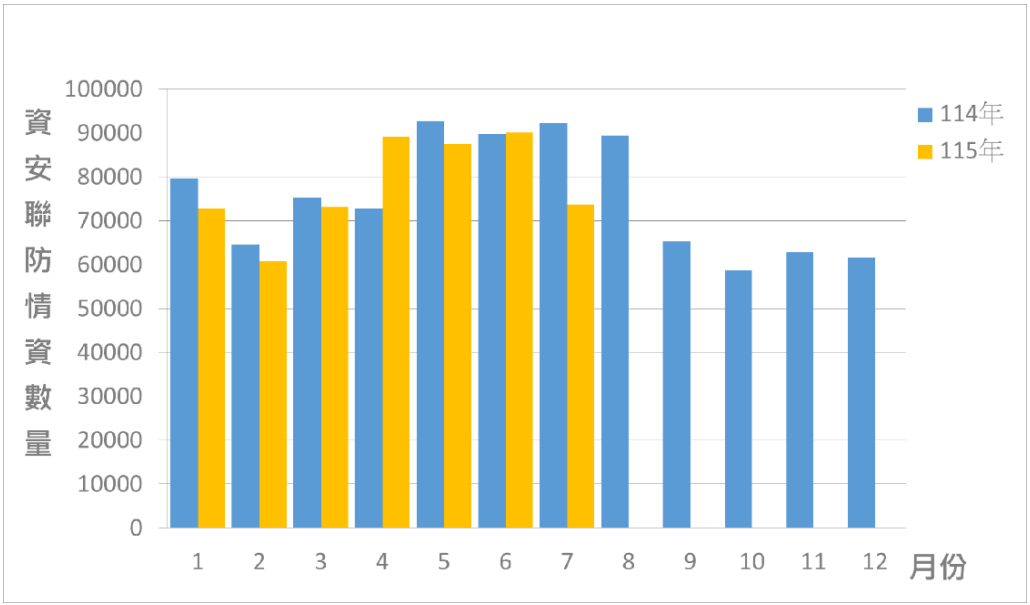

圖 2 資安聯防監控情資統計

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 LxBase RAT 以竊取電腦機敏資訊，LxBase RAT 是一種資訊竊取遠端操控木馬，竊取資料範圍涵蓋瀏覽器資料、數位錢包及社群平台帳號密碼等，其包含複雜規避檢測手法，除了竊取本機資訊外，亦具備下載後續更多惡意程式之功能，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 145 件（包含攻防演練數量 62 件），為去年同期的 0.62 倍，通報類型以非法入侵為主，占本月通報件數 62.07%。本

月發現駭客利用 OpenClaw、Hermes Agent 等開源 AI Agent 針對政府網站進行攻擊，包括雲端服務遭駭導致資料外洩，亦有個別網站既有弱點遭利用，包括 SQL Injection、路徑遍歷及任意檔案下載等情形。近 1 年資安事件通報統計詳見圖 3。

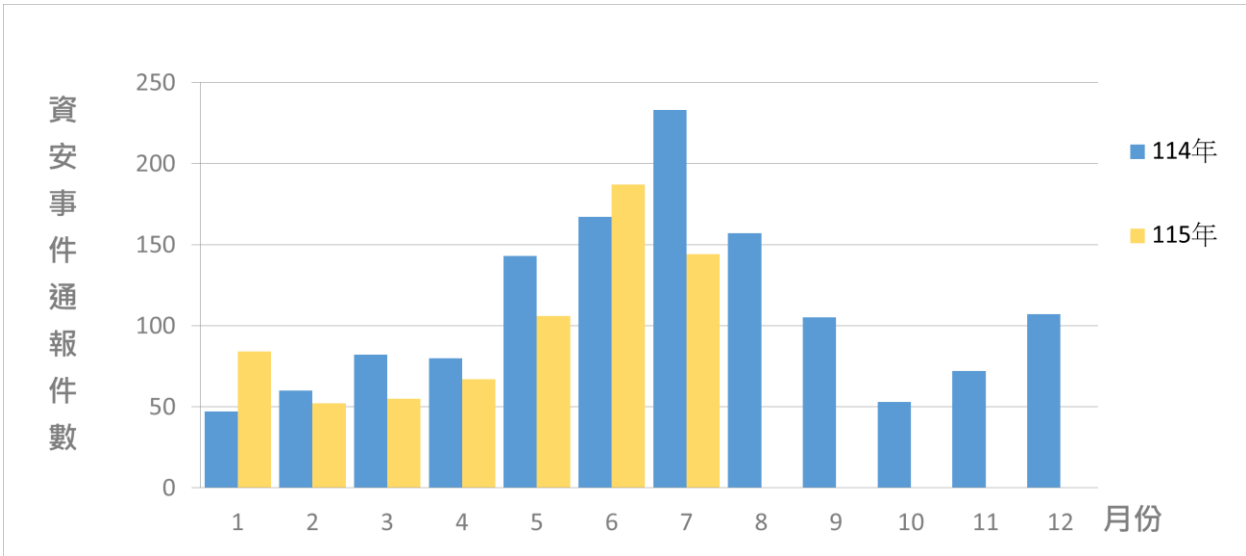

圖 3 資安事件通報統計

(二) 重要漏洞資訊，詳請參考附錄。

五、國際資安新聞

「GhostApproval（幽靈授權）」技術可誘騙 AI 程式編碼工具修改沙盒外部檔案

（資料來源：SC Media）

資安公司 Wiz 近期揭露了一項名為「GhostApproval」的新型資安威脅。研究指出，駭客能透過誘騙 AI 程式編碼助理，去修改工作區（workspace）以外的檔案，進而對用戶系統構成安全威脅。該技術的概念

驗證（Proof of Concept，PoC）濫用了符號連結（symlinks）。攻擊者利用專案中的說明文件（README），指示 AI 去編輯儲存庫（repo）內的特定檔案，然而，該檔案其實是一個「符號連結」，悄悄指向受害者電腦沙盒（sandbox）防護之外的重要機密檔案。攻擊者能藉此將惡意 SSH 金鑰寫入受害者的系統設定，從而直接奪取系統的存取權限。

研究人員測試 6 款主流的 AI 編碼助理，包含 Amazon Q Developer、Anthropic Claude Code、Augment Code、Cursor、Google Antigravity 以及 Windsurf，結果發現它們全部都存在此漏洞。在報告發表時，AWS、Anthropic、Cursor 和 Google 已針對該缺陷發布修正，而 Windsurf 的報告仍在等待中、Augment Code 不認為 GhostApproval 是漏洞。相關廠商建議用戶應盡快將軟體更新至最新版本，或確認系統已自動完成修復，以確保資訊安全。

ServiceNow 嚴重程式碼執行漏洞，現已遭實際攻擊利用

（資料來源：Bleeping Computer）

威脅情報公司 Defused 指出，企業愛用的 ServiceNow AI 平臺存在重大安全漏洞（編號 CVE-2026-6875），且自 7 月 19 日起已遭駭客實際利用。該漏洞由 Searchlight Cyber 於 4 月 1 日發現，允許未經身分驗證的攻擊者逃脫沙箱並在平台內遠端執行惡意程式。攻擊者正以不同的手法，鎖定仍是原始概念驗證（PoC）報告中所提到的同一個未經身分驗證

接收點（pre-auth sink）。

由於《富比士》500 強（Fortune 500）企業中多數都使用 ServiceNow 平臺處理業務，該漏洞恐引發高複雜度的資安攻擊，進而危及企業核心工作流程，並可能影響敏感的業務資料。雖然 ServiceNow 官方尚未在公告中將其列為活躍攻擊目標，但其實際風險已不容忽視。ServiceNow 已於 4 月發布針對代管實例（hosted instances）的修復程式，並於 7 月 13 日發布針對自建主機（self-hosted instances）的修復程式，建議所有客戶立即將系統升級至最新版本，以防止企業核心資料遭受侵害。

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** Apache HTTP Server **嚴重程度：** （CVE-2026-23918：CVSS 8.8） （CVE-2026-29167：CVSS 9.8） （CVE-2026-44631：CVSS 9.8）	● 研究人員發現 Apache HTTP Server 存在記憶體雙重釋放、釋放後使用及緩衝區下溢等高風險漏洞。 ● 最嚴重情況可能使遠端攻擊者執行任意程式碼；受影響範圍包含 2.4.0 至 2.4.67 版本。 ● 官方已釋出修補版本，建議儘速更新至 Apache HTTP Server 2.4.68（含）以上版本。
	虛擬化平台 VMware ESX、vCenter、Workstation 與 Fusion **嚴重程度：** （CVE-2026-59309：CVSS 9.8） （CVE-2026-59310：CVSS 9.8） （CVE-2026-47876：CVSS 9.3）	● 研究人員發現 VMware ESX、vCenter、Workstation 與 Fusion 存在多項重大安全漏洞，影響多種政府與企業常用之虛擬化基礎架構。 ● 未經身分鑑別且可連線至 vCenter 之攻擊者可繞過驗證或執行任意程式碼；另具虛擬機器本機管理權限者亦可能透過 VMXNET3 於 ESX 主機執行程式碼。 ● 建議將 VMware ESX、vCenter、Workstation 等產品更新至官方指定版本。
	資料收集與分析平台 Splunk Enterprise、Splunk Cloud Platform 與 Splunk Secure Gateway **嚴重程度：** （CVE-2026-20251：CVSS 8.8）	● 研究人員發現 Splunk Secure Gateway App 存在不安全反序列化漏洞。 ● 不具 admin 或 power 角色之低權限使用者，可透過 App Key Value Store 的特製資料重建任意 Python 物件，進而執行任意程式碼。 ● 建議將 Splunk Enterprise 及 Splunk Secure Gateway 更新至官方指定版本；無法立即更新者可暫時停用或移除該

警訊	類別	內容說明
		App。
已知遭駭客利用之漏洞	**安全存取閘道設備** SonicWall SMA1000 系列產品 **嚴重程度：** （CVE-2026-15409：CVSS 10.0）	● CISA 已於 2026 年 7 月將 CVE-2026-15409 列入 KEV 清單，SonicWall 官方確認該漏洞已有利用情形。 ● SMA1000 Appliance Workplace 介面存在伺服器端請求偽造（SSRF）漏洞，未經身分鑑別之遠端攻擊者可發出非預期請求。 ● 官方已釋出修補版本，建議儘速更新至 12.4.3-03453 或 12.5.0-02835（含）以上版本。
	協作與文件平台 Microsoft Office SharePoint **嚴重程度：** （CVE-2026-50522：CVSS 9.8）	● CISA 已於 2026 年 7 月將 CVE-2026-50522 列入 KEV 清單，且該漏洞已有實際利用情形。 ● Microsoft Office SharePoint 存在不安全反序列化漏洞，未經身分鑑別之遠端攻擊者可透過網路執行任意程式碼。 ● 官方已釋出修補版本，建議將 Microsoft SharePoint Server Subscription Edition、Server 2019 或 Enterprise Server 2016 等系列產品更新至官方指定版本。
	企業通訊與協作平台 Cisco Unified Communications Manager 與 Unified CM SME **嚴重程度：**	● CISA 已於 6/25 將 CVE-2026-20230 列入 KEV 清單，Cisco 亦於 7/1 更新公告正式確認該漏洞已遭實際利用。 ● 當 WebDialer 服務啟用時，未經身分鑑別之遠端攻擊者可透過特製 HTTP 請求進行伺服器端請求偽造（SSRF），寫入作業系統檔案並可能提升至 root 權限。

警訊	類別	內容說明
	（CVE-2026-20230：CVSS 8.6）	● 官方已提供修補版本，Release 14 請更新至 14SU6；Release 15 請套用對應 COP，或於 15SU5 發布後完成更新。修補前可評估暫時停用 WebDialer 服務。
	資安管理系統 Check Point Security Management Server 與 Multi-Domain Security Management Server **嚴重程度：** （CVE-2026-16232：CVSS 9.1）	● CISA 已將 CVE-2026-16232 列入 KEV 清單，Check Point 官方已觀察到少數實際利用案例。 ● 未經身分鑑別之遠端攻擊者可取得應用程式登入 Token，並透過 SmartConsole 以完整管理員權限登入管理伺服器，進而修改安全政策及系統組態。 ● 官方已提供修補版本，請依官方建議套用修補程式，且更新前避免將管理介面直接暴露於網際網路。

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。