

TWCERT/CC 資安情資電子報

2026 年 6 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在數位發展部指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組 織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 4 章節：

第1章、封面故事：本月TWCERT/CC所發布之資安情資中，官網點閱次數最高之情資列為本月份封面故事。

第2章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇可能包含資訊安全宣導、資安趨勢、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟硬體系統資安議題、軟硬體漏洞資訊、新興應用資安及資安小知識。

第3章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第4章、TVN漏洞公告：TWCERT/CC為CVE編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明本月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN)平台其CVSS 3分數為8.8以上之漏洞。

目錄

內容

目錄 II

第 1 章、封面故事 1

旅遊 eSIM 的陷阱：流量路徑不揭露，出差人員連線資料恐暴露境外 1

第 2 章、國內外重要資安事件 6

2.1 資安趨勢 6

2.1.1 知名開源框架 TanStack 遭「Mini Shai-Hulud」供應鏈攻擊，開源安全風險受關注 6

2.2 軟硬體系統資安議題 10

2.2.1 「FortiBleed」大規模憑證竊取行動：企業防火牆與VPN設備面臨風險 10

2.3 軟硬體漏洞資訊 13

2.3.1 PostgreSQL存在11個高風險安全漏洞，請儘速確認並進行修補 13

2.3.2 Oracle針對旗下多款產品發布重大資安公告 15

2.3.3 Palo Alto Networks PAN-OS存在重大資安漏洞(CVE-2026-0257) 19

2.3.4 Ivanti Neurons for ITSM存在高風險資安漏洞(CVE-2026-9614) 21

2.3.5 Ivanti旗下Sentry存在2個重大資安漏洞 22

2.3.6 Veeam旗下Veeam Backup & Replication備份軟體存在重大資安漏洞(CVE-2026-44963) 23

2.3.7 Oracle PeopleSoft PeopleTools 存在重大資安漏洞(CVE-2026-35273) 24

2.3.8 Fortinet旗下FortiSandbox、FortiSandbox Cloud 和 FortiSandbox PaaS存在重大資安漏洞(CVE-2026-25089) 25

2.3.9 SAP針對旗下多款產品發布重大資安公告 26

2.3.10 Check Point 旗下 Security Gateways 與 Spark Firewalls 存在重大資安漏洞(CVE-2026-

50751) 28
2.3.11 Oracle針對旗下多款產品發布重大資安公告 29
2.3.12 Fortinet 防火牆等設備遭受憑證竊取攻擊，請儘速確認並修補 30
2.3.13 Cisco 旗下身分識別服務存在重大資安漏洞(CVE-2026-20181) 31
第 3 章、資安研討會及活動 32
第 4 章、TVN 漏洞公告 42
編輯：TWCERT/CC 團隊 44

第 1 章、封面故事

旅遊 eSIM 的陷阱：流量路徑不揭露，出差人員連線資料恐暴露境外



美國東北大學研究團隊於 2025 年資安學術研討會 USENIX Security Symposium 發表實證研究報告《eSIMplicity or eSIMplification? Privacy and Security Risks in the eSIM Ecosystem》，針對數十款市售旅遊 eSIM 進行實際測試，發現多數旅遊 eSIM 採用Home-Routed Roaming（HRR）架構，使用者流量不會從當地網路直接出口，而是先回送至本籍網路（Home Network）業者的核心設施處理後才連上目的地服務。部分業者

的本籍網路位於中國，因此使用者的流量會先經過中國電信業者的基礎設施。在 HRR 架構下，本籍網路可完整看到連線時間戳記、來源位置、DNS 查詢紀錄及所存取的服務端點，即使傳輸層已採用 TLS 加密，這些連線層級的紀錄仍可被側錄，且業者通常不會主動於商品頁面揭露相關資訊。

多款eSIM流量繞送中國電信業者基礎設施

研究團隊透過 traceroute 與 IP 地理位置資料庫交叉比對，確認多款 eSIM 的 Public IP 出口地點與使用者所在地不符。以登記於愛爾蘭的Holafly為例，流量實際經由中國移動國際的香港節點對外連線，Public IP 顯示在中國境內，其訂閱管理伺服器（Subion Manager Data Preparation，SM-DP+，負責準備 eSIM 設定檔並使其可供使用者裝置下載的後端基礎設施）位址亦屬中國移動網路，代表 eSIM 設定檔的下載與管理流程本身亦由中國移動控制。

研究亦發現部分 eSIM 設定檔內嵌 SIM Application Toolkit（STK）指令，可在使用者不介入操作的情況下主動發起資料連線或接收簡訊。研究人員觀察到特定 eSIM在使用者不知情的情況下，透過設定檔主動連線至境外伺服器，並接收來自香港號碼的簡訊。

旅遊 eSIM 轉售商可追蹤用戶位置並向裝置植入惡意指令

成為轉售商的門檻極低，旅遊 eSIM 市場存在大量轉售商，轉售商本身不擁有電信基礎設施，僅向行動網路業者（MNO，Mobile Network Operator） 或行動虛擬網路業者（MVNO，Mobile Virtual Network Operator）批發設定檔後轉賣。

研究指出，研究人員實際開設帳號後發現，轉售商可透過 API 存取啟用中使用者的國際行動用戶識別碼（IMSI，International Mobile

Subscriber Identity）、行動用戶號碼（MSISDN）及裝置位置（精確度可達約 0.8 公里），並具備向使用者裝置發送二進位簡訊（binary SMS）的能力。binary SMS 是一種不會顯示在使用者簡訊收件匣、直接由作業系統處理的特殊訊息格式，可用於修改裝置設定、觸發特定應用程式行為，或作為植入惡意程式及維持遠端控制的管道，此類訊息可修改裝置設定或植入惡意程式。部分平台更允許轉售商為使用者裝置分配靜態 Public IP，使裝置可從外部網路直接存取，存在遭遠端惡意連線的風險。

對企業與組織的資安影響

出差人員若以 HRR 架構的旅遊 eSIM 存取網路服務，所有資料流量將途經本籍網路業者的核心設施處理。研究指出，本籍網路在此過程中可完整看到使用者連上了哪些服務、何時連線、從哪個位置連線，以及應用程式的使用情況，本籍網路亦可透過拜訪網路與本籍網路之間的訊號交換，推算使用者的大略位置。即使傳輸層已加密，這些連線層級的後設資料仍可被本籍網路側錄。

研究進一步指出，本籍網路往往是使用者完全不知情的境外第三方業者，使用者難以判斷其通訊資料究竟流經哪個法律管轄區，以及由哪個組織負責管理。部分旅遊 eSIM 的 SM-DP+ 伺服器與本籍網路屬同一境外業者，代表 eSIM 設定檔的下載與管理流程本身亦在該業者的控制範圍內，而非僅限於上網流量。

除上述架構性風險外，研究實測亦發現 eSIM 設定檔管理本身存在設計脆弱性。刪除設定檔時若裝置處於離線狀態，刪除通知將無法送達 SM-DP+ 伺服器，伺服器因此仍視該設定檔為啟用中，使用者以原 QR Code 重新安裝時將收到「已安裝」錯誤而遭拒，須聯繫業者手動重置方可恢復使用。研究亦指出，攻擊者可藉由攔截刪除設定檔過程中的網

路連線，使刪除通知無法送達伺服器，進而封鎖使用者重新安裝設定檔的能力（圖1）。

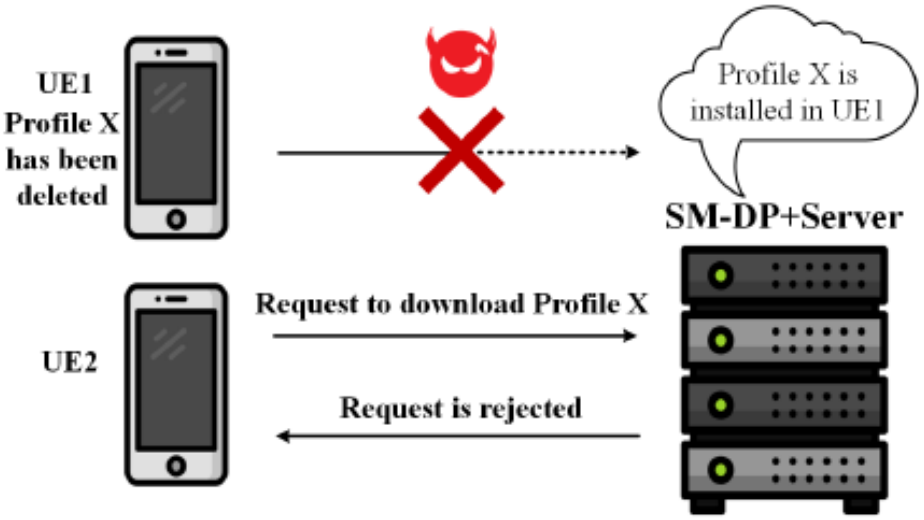


圖2：eSIM 設定檔刪除通知遭攔截示意圖。資料來源（Motallebighomi et al., eSIMplicity or eSIMplification? Privacy and Security Risks in the eSIM Ecosystem, USENIX Security 2025）

防護建議

1. 建立差旅行動上網政策：制定可使用的 eSIM 業者白名單，要求業者揭露合作電信商名稱、IP 出口地區及資料處理地點。對高風險職務人員應禁止使用未經審核的旅遊 eSIM 存取內部資源。「免 VPN 可使用境外服務」通常代表流量透過境外節點達成，不得作為安全評估依據。
2. 出差期間敏感系統存取強制 VPN：存取公務信箱、內部系統或視訊會議時，一律透過企業核准的 VPN 或零信任網路存取（ZTNA，Zero Trust Network Access）架構連線，確保流量經由

受控通道傳輸。

3. 監控帳號異常登入並強制多重要素驗證（MFA，Multi-Factor Authentication）：設定境外 IP 登入告警規則，出現中國、香港等地區登入紀錄時立即觸發通報。確認 MFA 已正確啟用，並定期審查登入紀錄。

- 相關連結
  1. eSIMplicity or eSIMplification? Privacy and Security Risks in the eSIM Ecosystem
  2. ENISA, Embedded SIM Ecosystem, Security Risks and Measures

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 知名開源框架 TanStack 遭「Mini Shai-Hulud」供應鏈攻擊，開源安全風險受關注



知名網頁應用程式框架 TanStack 的 npm 套件近期遭到駭客組織 TeamPCP 發動名為「Mini Shai-Hulud」的大規模軟體供應鏈攻擊，攻擊者在短短幾分鐘內發布了 42 個 「@tanstack/*」套件的 84 個惡意版本。本次攻擊的惡意套件首次具備有效的 SLSA（軟體供應鏈安全框架）第3級來源證明，使其外觀與合法套件無異。該惡意軟體具備自我傳播能力，

已迅速擴散至 Mistral AI、UiPath 與 OpenSearch 等 170 多個 npm 與 PyPI 套件，更導致知名 AI 企業 OpenAI 內部員工裝置遭入侵，部分原始碼專案庫遭未經授權存取。

根據 TanStack 官方發布的事後檢討報告，這次的攻擊之所以能成功，根本原因在於駭客將三個獨立的弱點串聯在一起，官方特別強調，這三項弱點「缺一不可」，單一弱點皆不足以構成此次的攻擊。以下是根據 TanStack 官方報告重新整理的三項弱點剖析：

1. 外部Pull Request（PR）可在主專案庫環境執行

官方的「bundle-size.yml」工作流程使用「pull_request_target」觸發條件處理外部Pull Request（PR）請求，並在主專案庫的工作流程環境下檢出與執行外部程式碼，使不受信任的可能接觸主專案庫的相關資源。儘管官方在設計工作流程時，曾試圖透過設定唯讀權限區分信任邊界，卻忽略兩個致命的機制盲點。首先，GitHub Actions 的快取機制在寫入快取時，使用的是執行器內部的Token，因此不受工作流程唯讀權限限制；其次，快取範圍是專案庫共享，表示主專案庫上下文中執行的外部PR請求程式碼，將能夠越權竄改並污染主專案庫的快取資料。

2. 低權限測試流程與高權限發布流程共用快取

駭客在外部PR請求中夾帶特定的惡意腳本（vite_setup.mjs），將惡意資料寫入pnpm的儲存目錄中，並使用與官方發布流程（release.yml）相同的快取金鑰。當該PR請求建置測試任務結束後，包含惡意程式的資料即被寫入 GitHub Actions 的共用快取中。遭植入惡意內容的快取可能持續保留於系統中，直到專案將其他合法程式碼合併至主分支，並觸發「release.yml」發布工作流程。執行過程中，「設定工具」步驟可能自動載入並還原該快取檔案，使惡意內容進入原具有較高信任權限的發布

流程。

3. 發布流程授予 OIDC Token 權限，但缺乏足夠的執行環境隔離

為了能夠透過 OIDC 信任綁定在 npm 上發布套件，官方的「release.yml」發布工作流程宣告「id-token: write」權限，然而，這項權限卻遭到駭客濫用。當被投毒的快取在執行器上還原後，駭客潛伏的惡意二進制檔案便會在建置步驟中被觸發，這些惡意程式會主動尋找 GitHub Actions 執行器的工作處理程序，藉由讀取該程序的記憶體配置，直接從中提取出動態生成的 OIDC Token。取得OIDC Token後，惡意程式便越權直接向 npm 註冊表發送 POST 請求發布惡意套件，此舉完全繞過了官方工作流程中原先設定好的「發布套件」步驟。

此次供應鏈攻擊影響範圍甚大，不僅導致跨領域開源生態系淪陷，包含每週下載量破千萬的「@tanstack/react-router」在內的 42 個套件受害，惡意軟體入侵開發者裝置後，還會自動搜尋並利用受害者權限發布其他套件，使災情擴大至「@mistralai」、「@uipath」、「@opensearch-project」等超過 170 個專案。在感染後，名為「router_init.js」的惡意酬載會進行大範圍憑證竊取，全面搜刮 CI/CD 環境與開發者本機的機敏資料。這些資料並未傳送至傳統的 C2 惡意中繼站，而是隱蔽地透過點對點（P2P）資料外洩，經由去中心化的 Session 通訊網路進行端到端加密傳輸，使流量偽裝成一般的通訊軟體遙測數據。更具威脅的是，該惡意軟體內建系統刪除機制，會持續監控遭竊的 GitHub Token有效狀態；若偵測到Token已遭撤銷，便會立即觸發系統指令，將受害者的主目錄資料刪除。

TWCERT/CC 呼籲開發團隊與企業應立即檢視內部專案，並採取以下應變措施：

1. 清查受害範圍：立即檢查專案的 lockfile 與 CI 日誌，確認是否安裝受影響或遭竄改的版本套件。
2. 優先清除常駐程式：在撤銷任何外洩的Token之前務必先檢查 macOS 或 Linux 系統中是否存在 gh-token-monitor 常駐程式並將其移除，以避免觸發惡意軟體的資料刪除機制。
3. 全面更換機敏憑證：請立即更換可能曝險在受感染環境中的所有憑證，包含 GitHub/npm Token、雲端供應商憑證、SSH 金鑰等。
4. 強化 CI/CD 與 OIDC 工作流程：嚴格審查 GitHub Actions，避免在處理來源不明或不受信任的Pull Request（PR）時，使用「pull_request_target」作為觸發條件，並禁止此類工作流程具備寫入快取的權限；此外，應落實 OIDC Token的最小權限原則，僅在需要發布套件的特定步驟授予權限。
5. 勿單一依賴 SLSA 證明：此次事件證明，具備 SLSA 來源證明的套件亦可能含有惡意程式碼。建議企業在導入套件時，應結合安裝時的行為監控與套件發布時間緩衝期（Cooldowns）機制，以多層次防禦降低供應鏈風險。

- 相關連結
  1. Postmortem: TanStack npm supply-chain compromise
  2. Malware in 42 @tanstack/* packages exfiltrates cloud credentials, GitHub tokens, and SSH keys
  3. TanStack Npm Packages Compromised Inside The Mini Shai Hulud Supply Chain Attack
  4. TanStack npm Packages Compromised in Ongoing Mini Shai-Hulud Supply-Chain Attack
  5. TeamPCP's Mini Shai-Hulud Is Back

2.2 軟硬體系統資安議題

2.2.1 「FortiBleed」大規模憑證竊取行動：企業防火牆與VPN設備面臨風險



威脅情報平台 InfoStealers 近日揭露名為「FortiBleed」的大規模憑證外洩事件，全球約7.5萬台 FortiGate防火牆與 VPN 閘道設備的登入憑證可能已遭竊取。資安研究人員估計，受影響設備約占全球對外暴露 Fortinet 設備的一半，涉及範圍涵蓋跨國企業、政府機構及關鍵基礎設施等組織。

報告指出，此波名為「FortiBleed」的憑證竊取活動，疑似與俄語系網路犯罪集團有關。研究人員分析，攻擊者曾針對逾32萬台 FortiGate設備發動約11.6億次登入憑證嘗試，並對超過16萬台Microsoft SQL Server (MSSQL) 伺服器進行約21億次暴力破解。顯示其具備大規模掃描、憑證驗證及自動化攻擊能力。

除嘗試使用過往外洩或未定期更換的帳號密碼，該集團還主動攔截 SSL VPN 驗證雜湊值，並透過由45個GPU組成、使用Hashtopolis管理的大型叢集進行離線破解。成功取得有效憑證後，攻擊者可能進一步橫向移動至內部 Active Directory 環境，藉此建立並維持長期存取權限。惟目前公開資訊尚未完整說明相關設備設定檔及驗證雜湊值的最初取得途徑，因此實際受影響原因可能包含歷史事件外洩資料遭重新利用、弱密碼遭破解、管理介面暴露於網際網路，以及設備設定檔遭未授權取得等多種情況。

研究人員認為，此次事件的影響可能與舊版憑證雜湊機制有關。儘管Fortinet 早在2025年初便將管理員憑證雜湊演算法從 SHA-256 升級為更安全的 PBKDF2，但更新後須重新登入才能生效，導致許多設備仍採用較脆弱的舊版格式儲存憑證。一旦設定檔外洩，攻擊者即可離線進行暴力破解，大幅提高憑證遭破解的風險。

針對此波攻擊，Fortinet表示，目前未發現事件涉及新的 FortiOS 弱點，相關資料可能包含過往資安事件取得的憑證，以及透過暴力破解方式取得的帳號密碼。未定期更換憑證、使用弱密碼，或未啟用多因子驗證（MFA）的設備，可能面臨較高風險。Fortinet 已持續調查相關情形，並主動聯繫可能受影響的客戶提供協助。

為降低憑證遭濫用及設備遭未授權存取的風險，確保企業與組織的網路安全，建議企業管理團隊採取以下應變措施：

1. 終止連線並重設密碼：中斷所有進行中的管理員工作階段，全面重設 Fortinet VPN 與管理員帳號的密碼，並強制落實高強度的密碼政策。
2. 全面啟用多因子驗證（MFA）：務必為所有管理員帳號及 VPN

使用者帳號啟用 MFA，以有效防範憑證外洩風險。

3. 升級 FortiOS 並確認密碼雜湊格式：將設備升級至支援 PBKDF2 演算法的最新版本。同時，應依官方建議移除舊版加密設定。
4. 檢視設備帳號與設定內容：檢查防火牆、VPN 使用者名單及其他設定是否遭未經授權的竄改，並盡可能與已知安全的設定檔進行比對。需特別留意系統中是否暗藏不明帳號，例如「forticloud」、「fortiuser」、「fortinet-support」或「fortinet-tech-support」等。
5. 檢視登入與系統活動紀錄：檢視管理員登入紀錄，確認是否有來自未知 IP 位址的意外存取行為；同步查閱網域控制器日誌，積極防堵橫向移動、異常存取、可疑帳號活動及未經授權的設定變更。
6. 限制管理介面的公開存取：盡速確認設備管理介面是否暴露於網際網路，建議將管理介面從公開網際網路移除，僅允許受信任的 IP 或透過跳板機/ VPN 方式存取。
7. 調查可能的後續入侵活動：如發現異常登入、未知帳號或設定遭竄改，應立即啟動事件調查，確認是否涉及內部系統、帳號或資料遭未授權存取。

- 相關連結

1. FortiBleed: 75,000 Fortinet Firewalls Compromised
2. Analysis of Reported Credential Compromise of FortiGate Devices
3. CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure
4. Hudson Rock's FortiBleed Checker

2.3 軟硬體漏洞資訊

2.3.1 PostgreSQL存在11個高風險安全漏洞，請儘速確認並進行修補

CVE 編號	CVE-2026-6472~CVE-2026-6479,CVE-2026-6575,CVE-2026-6637,CVE-2026-6638
影響產品	PostgreSQL
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下： https://www.postgresql.org/about/news/postgresql-184-1710-1614-1518-and-1423-released-3297/

- 內容說明：

  研究人員發現 PostgreSQL 存在 11 個高風險安全漏洞(CVE-2026-6472 至 CVE-2026-6479、CVE-2026-6575、CVE-2026-6637 及 CVE-2026-6638)，類型包含堆疊型緩衝區溢位(Stack-based Buffer Overflow)、SQL 注入(SQL Injection)及整數迴繞(Integer Wraparound)等，最嚴重可使取得一般權限之遠端攻擊者執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - PostgreSQL 14 版本
  - PostgreSQL 15 版本
  - PostgreSQL 16 版本
  - PostgreSQL 17 版本
  - PostgreSQL 18 版本
- 資料來源：
  1. PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 Released!
  2. CVE-2026-6472
  3. CVE-2026-6473
  4. CVE-2026-6474

5. CVE-2026-6475
6. CVE-2026-6476
7. CVE-2026-6477
8. CVE-2026-6478
9. CVE-2026-6479
10. CVE-2026-6575
11. CVE-2026-6637
12. CVE-2026-6638

2.3.2 Oracle針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2026-46833,CVE-2026-46840,CVE-2026-46775,CVE-2026-46839,CVE-2026-2332,CVE-2026-33557,CVE-2025-15467,CVE-2026-41044,CVE-2026-46822,CVE-2026-46824,CVE-2026-46817,CVE-2026-46819,CVE-2026-46837,CVE-2026-46826,CVE-2026-46827,CVE-2026-34311
影響產品	Oracle Database Server、REST Data Services、Communications Unified Assurance、iAssets、Universal Work Queue、Payments、Internet Procurement Connector、Flow Manufacturing、Payroll、Hospitality OPERA 5 Property Services
解決辦法	根據官方網站釋出的解決方式進行修補：https://www.oracle.com/security-s/cspumay2026.html

- 內容說明：

【CVE-2026-46833，CVSS：9.0】

此漏洞存在於 Oracle Database Server 的 Net Service 元件，允許未經身分驗證的攻擊者透過 TLS 存取 Net Service 元件，可能對其他產品造成重大影響。

【CVE-2026-46840，CVSS：10.0】

此漏洞存在於 Oracle REST Data Services 的 Backend-as-a-Service 元件，允許未經身分驗證的攻擊者透過 HTTPS 網路存取 Oracle REST Data Services。

【CVE-2026-46775，CVSS：9.9、CVE-2026-46839，CVSS：9.9】

此漏洞存在於 Oracle REST Data Services 的 Core 元件，低權限的攻擊者可透過 HTTPS 網路存取 Oracle REST Data Services，若成功利用可能導致 Oracle REST Data Services 被完全控制。

【CVE-2026-2332，CVSS：9.1】

此漏洞存在於 Oracle REST Data Services 的 Core (Eclipse Jetty)元件，允許未經身分驗證的攻擊者透過 HTTPS 網路存取 Oracle REST Data Services，若成功利用可能導致未經授權新增、刪除或修改關鍵數據。【CVE-2026-33557，CVSS：9.1】

此漏洞存在於 Oracle Communications Unified Assurance 的 Message Bus (Apache Kafka)元件，允許未經身分驗證的攻擊者透過 TCP 網路存取 Oracle Communications Unified Assurance，若成功利用可能導致未經授權新增、刪除或修改關鍵數據。【CVE-2025-15467，CVSS：8.8】

此漏洞存在於 Oracle Communications Unified Assurance 的 Core (MySQL Server)元件，允許未經身分驗證的攻擊者透過 HTTP 網路存取 Oracle Communications Unified Assurance。若要成功利用此漏洞需仰賴除攻擊者之外的其他使用者互動。【CVE-2026-41044，CVSS：8.8】

此漏洞存在於 Oracle Communications Unified Assurance 的 Message Bus (Apache Kafka)元件，低權限的攻擊者可透過 HTTPS 網路存取 Oracle Communications Unified Assurance，若成功利用可能導致 Oracle Communications Unified Assurance 被完全控制。【CVE-2026-46822，CVSS：9.9】

此漏洞存在於 Oracle iAssets 的 Internal Operations 元件，低權限的攻擊者可透過 HTTPS 網路存取 Oracle iAssets 並使其遭受攻擊，若成功利用可能導致 Oracle iAssets 被完全控制。【CVE-2026-46824，CVSS：9.9】

此漏洞存在於 Oracle Universal Work Queue 的 Work Provider Site Level Administration 元件，低權限的攻擊者可透過 HTTPS 網路存取 Oracle

Universal Work Queue，若成功利用可能導致 Oracle Universal Work Queue 被完全控制。

【CVE-2026-46817，CVSS：9.8】

此漏洞存在於 Oracle Payments 的 File Transmission 元件，允許未經身分驗證的攻擊者透過 HTTP 網路存取 Oracle Payments，若成功利用可能導致 Oracle Payments 被完全控制。

【CVE-2026-46819，CVSS：9.1】

此漏洞存在於 Oracle Internet Procurement Connector 的 Internal Operations 元件，允許未經身分驗證的攻擊者透過 HTTP 網路存取 Oracle Internet Procurement Connector，若成功利用可能導致未經授權新增、刪除或修改關鍵數據。

【CVE-2026-46837，CVSS：8.8】

此漏洞存在於 Oracle Flow Manufacturing 的 Security 元件，低權限的攻擊者可透過 SQL 存取網路，若成功利用可能導致 Oracle Flow Manufacturing 被完全控制。

【CVE-2026-46826，CVSS：8.8】

此漏洞存在於 Oracle Payroll 的 Internal Operations 元件，低權限的攻擊者可透過 HTTPS 網路存取，若成功利用可能導致 Oracle Payroll 被完全控制。

【CVE-2026-46827，CVSS：8.8】

此漏洞存在於 Oracle Payroll 的 Self Service Manager 元件，低權限的攻擊者可透過 HTTP 網路存取，若成功利用可能導致 Oracle Payroll 被完全控制。

【CVE-2026-34311，CVSS：9.8】

此漏洞存在於 Oracle Hospitality OPERA 5 Property Services 的 Opera 元件，允許未經身分驗證的攻擊者透過 HTTP 網路存取 Oracle

Hospitality OPERA 5 Property Services，若成功利用可能導致 OPERA 5 Property Services 被完全控制。

- 影響平台：

【CVE-2026-46833】

- Oracle Database Server 23.4.0 至 23.26.2 版本

【CVE-2026-46840、CVE-2026-46775、CVE-2026-46839、CVE-2026-2332】

- Oracle REST Data Services 24.2.0 至 26.1.0 版本

【CVE-2026-33557、CVE-2025-15467、CVE-2026-41044】

- Oracle Communications Unified Assurance 6.11 至 7.00 版本

【CVE-2026-46822】

- Oracle iAssets 12.2.3 至 12.2.15 版本

【CVE-2026-46824】

- Oracle Universal Work Queue 12.2.3 至 12.2.15 版本

【CVE-2026-46817】

- Oracle Payments 12.2.3 至 12.2.15 版本

【CVE-2026-46819】

- Oracle Internet Procurement Connector 12.2.3 至 12.2.15 版本

【CVE-2026-46837】

- Oracle Flow Manufacturing 12.2.3 至 12.2.15 版本

【CVE-2026-46827、CVE-2026-46826】

- Oracle Payroll 12.2.3 至 12.2.15 版本

【CVE-2026-34311】

- Oracle Hospitality OPERA 5 Property Services 5.6.19.24、
- Oracle Hospitality OPERA 5 Property Services 5.6.22、
- Oracle Hospitality OPERA 5 Property Services 5.6.25.19、
- Oracle Hospitality OPERA 5 Property Services 5.6.27.6、
- Oracle Hospitality OPERA 5 Property Services 5.6.28

- 資料來源：

1. Oracle Critical Security Patch Update Advisory - May 2026

2.3.3 Palo Alto Networks PAN-OS存在重大資安漏洞(CVE-2026-0257)

CVE 編號	CVE-2026-0257
影響產品	Palo Alto Networks PAN-OS、Prisma Access
解決辦法	根據官方網站釋出的解決方式進行修補： https://security.paloaltonetworks.com/CVE-2026-0257

- 內容說明：

  Palo Alto Networks 防火牆作業系統 PAN-OS 的 GlobalProtect 入口網站和通道設備存在身分驗證繞過漏洞，攻擊者可利用該漏洞繞過安全限制並建立未經授權的 VPN 連線。

- 影響平台：
  - PAN-OS 12.1.7(不含)以前版本
  - PAN-OS 11.2.4-h17(不含)以前版本
  - PAN-OS 11.2.7-h14(不含)以前版本
  - PAN-OS 11.2.10-h7(不含)以前版本
  - PAN-OS 11.2.12(不含)以前版本
  - PAN-OS 11.1.4-h33(不含)以前版本
  - PAN-OS 11.1.6-h32(不含)以前版本
  - PAN-OS 11.1.7-h6(不含)以前版本
  - PAN-OS 11.1.10-h25(不含)以前版本
  - PAN-OS 11.1.13-h5(不含)以前版本
  - PAN-OS 11.1.15(不含)以前版本
  - PAN-OS 10.2.7-h34(不含)以前版本
  - PAN-OS 10.2.10-h36(不含)以前版本
  - PAN-OS 10.2.13-h21(不含)以前版本
  - PAN-OS 10.2.16-h7(不含)以前版本
  - PAN-OS 10.2.18-h6(不含)以前版本
  - Prisma Access 11.2.7-h13(不含)以前版本

- Prisma Access 10.2.10-h36(不含)以前版本

- 資料來源：
  1. CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities
  2. CVE-2026-0257

2.3.4 Ivanti Neurons for ITSM存在高風險資安漏洞(CVE-2026-9614)

CVE 編號	CVE-2026-9614
影響產品	Ivanti Neurons for ITSM
解決辦法	根據官方網站釋出的解決方式進行修補： https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2026-9614?language=en_US

- 內容說明：

  ITSM 是 Ivanti 旗下一款可靠且強大 IT 服務管理的解決方案，可協助組織提升服務效率，確保 IT 營運合規及安全。近日針對 Ivanti Neurons for ITSM 發布重大資安公告(CVE-2026-9614，CVSS：8.8)，此漏洞可允許經身分驗證的遠端攻擊者取得系統管理存取權限。

- 影響平台：
  - Ivanti Neurons for ITSM (On-Premises) 2025.4(含)之前版本
  - Ivanti Neurons for ITSM (Cloud) 2026.1(含)之前版本
- 資料來源：
  1. Security Advisory Ivanti Neurons for ITSM (CVE-2026-9614)
  2. CVE-2026-9614

2.3.5 Ivanti旗下Sentry存在2個重大資安漏洞

CVE 編號	CVE-2026-10520,CVE-2026-10523
影響產品	Ivanti Sentry
解決辦法	請更新至以下版本： Ivanti Sentry 10.5.2(含)之後版本 Ivanti Sentry 10.6.2(含)之後版本 Ivanti Sentry 10.7.1(含)之後版本

- 內容說明：

  近日 Ivanti 針對旗下 Sentry 發布重大資安漏洞公告

  【CVE-2026-10520，CVSS：10.0】

  此漏洞為作業系統命令注入漏洞，允許未經身分驗證的遠端使用者以 root 權限執行遠端程式碼。

  【CVE-2026-10523，CVSS：9.9】

  此漏洞為身分驗證繞過漏洞，允許未經身分驗證的遠端攻擊者建立任意管理員帳號，並完全取得管理員權限。

- 影響平台：
  - Ivanti Sentry 10.5.1(含)以前版本
  - Ivanti Sentry 10.6.1(含)以前版本
  - Ivanti Sentry 10.7.0(含)以前版本
- 資料來源：
  1. Security Advisory Ivanti Sentry (CVE-2026-10520, CVE-2026-10523)
  2. CVE-2026-10520
  3. CVE-2026-10523

2.3.6 Veeam旗下Veeam Backup & Replication備份軟體存在重大資安漏洞(CVE-2026-44963)

CVE 編號	CVE-2026-44963
影響產品	Veeam Backup & Replication
解決辦法	請更新 Veeam Backup & Replication 至 12.3.2.4854(含)之後版本

- 內容說明：

  Veeam Backup & Replication 是 Veeam 核心備份軟體，近日 Veeam 發布重大資安漏洞公告，此漏洞(CVE-2026-44963，CVSS 4.x：9.4)允許經身分驗證的網域使用者，在備份伺服器上執行遠端程式碼(RCE)。

- 影響平台：
  - Veeam Backup & Replication 12.3.2.4465(含)之前 12 版本
- 資料來源：
  1. Vulnerability Resolved in Veeam Backup & Replication 12.3.2.4854
  2. CVE-2026-44963

2.3.7 Oracle PeopleSoft PeopleTools 存在重大資安漏洞(CVE-2026-35273)

CVE 編號	CVE-2026-35273
影響產品	Oracle PeopleSoft Enterprise PeopleTools
解決辦法	根據官方網站釋出的解決方式進行修補： https://www.oracle.com/security-s/-cve-2026-35273.html

- 內容說明：

  近日 Oracle 針對 PeopleSoft PeopleTools 發布重大資安公告(CVE-2026-35273，CVSS：9.8)，該漏洞允許未經身分驗證的遠端攻擊者可遠端程式碼執行。

- 影響平台：
  - PeopleSoft Enterprise PeopleTools 8.61、8.62 版本
- 資料來源：
  1. Oracle Security Alert Advisory - CVE-2026-35273
  2. CVE-2026-35273

2.3.8 Fortinet旗下FortiSandbox、FortiSandbox Cloud 和 FortiSandbox PaaS存在重大資安漏洞(CVE-2026-25089)

CVE 編號	CVE-2026-25089
影響產品	Fortinet FortiSandbox、FortiSandbox Cloud、FortiSandbox PaaS
解決辦法	請更新至以下版本： FortiSandbox 5.0.6(含)之後版本 FortiSandbox 4.4.9(含)之後版本 FortiSandbox Cloud 5.0.6(含)之後版本 FortiSandbox PaaS 5.0.6(含)之後版本

- 內容說明：

  Fortinet 旗下 FortiSandbox、FortiSandbox Cloud 和 FortiSandbox PaaS 的網頁介面存在缺少授權漏洞(CVE-2026-26089，CVSS：9.8)，可能允許未經身分驗證的攻擊者，透過 HTTP 請求執行未經授權的程式碼或命令。

- 影響平台：
  - FortiSandbox 5.0.0 至 5.0.5 版本
  - FortiSandbox 4.4.0 至 4.4.8 版本
  - FortiSandbox Cloud 5.0.4 至 5.0.5 版本
  - FortiSandbox PaaS 5.0.4 至 5.0.5 版本
- 資料來源：
  1. Second-Order OS Command Injection via JSON Input on start vnc feature
  2. CVE-2026-25089

2.3.9 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2026-40128,CVE-2026-27671,CVE-2026-44748
影響產品	SAP NetWeaver Application Server Java (Web Container)、NetWeaver AS ABAP and ABAP Platform
解決辦法	根據官方網站釋出的解決方式進行修補：https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2026.html

- 內容說明：

  【CVE-2026-40128，CVSS：9.0】

  SAP NetWeaver Application Server Java (Web Container)允許未經身分驗證的攻擊者，透過精心設計 HTTP 登入請求進而觸發路徑遍歷行為。

  【CVE-2026-27671，CVSS：9.8】

  由於 SAP NetWeaver AS ABAP and ABAP Platform 所使用的 RFC 協定驗證不足，未經身分驗證的攻擊者可透過精心設計的 RFC 請求，利用記憶體的邏輯錯誤進而損壞。

  【CVE-2026-44748，CVSS：9.9】

  SAP NetWeaver AS ABAP and ABAP Platform 允許具有普通權限且經身分驗證的攻擊者取得有效簽署訊息後，對簽署文件內容進行竄改後提交給驗證者。

- 影響平台：

  【CVE-2026-40128】

  - SAP NetWeaver Application Server Java (Web Container) Version(s) - ENGINEAPI 7.50

  【CVE-2026-27671】

  - SAP NetWeaver AS ABAP and ABAP Platform

Version(s) - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 722EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 91.9

【CVE-2026-44748】

- SAP NetWeaver AS ABAP and ABAP Platform
  Version(s) - SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816, SAP_BASIS 918, SAP_BASIS 919

- 資料來源：
  1. SAP Security Patch Day - June 2026
  2. CVE-2026-40128
  3. CVE-2026-27671
  4. CVE-2026-44748

2.3.10 Check Point 旗下 Security Gateways 與 Spark Firewalls 存在重大資安漏洞 (CVE-2026-50751)

CVE 編號	CVE-2026-50751
影響產品	Check Point Security Gateways、Spark Firewalls
解決辦法	根據官方網站釋出的解決方式進行修補： https://support.checkpoint.com/results/sk/sk185033

- 內容說明：

  Check Point 針對旗下產品 Security Gateways 與 Spark Firewalls 發布重大資安漏洞公告 (CVE-2026-50751，CVSS：9.3)。此漏洞允許未經身分驗證的遠端攻擊者利用 IKEv1 金鑰交換協議驗證邏輯缺陷，繞過使用者身分驗證，在無需有效密碼的情況下建立遠端存取 VPN 連線，進而存取內部資源或提升權限。

  備註：目前 Check Point 已觀察到有攻擊者利用此漏洞，建議儘速採取暫時緩解措施，以防止針對此漏洞可能的攻擊發生。

- 影響平台：
  - Security Gateways R82.10 Jumbo Hotfix Take 19 (含)之前版本
  - Security Gateways R82 Jumbo Hotfix Take 103 (含)之前版本
  - Security Gateways R81.20 Jumbo Hotfix Take 141 (含)之前版本
  - Security Gateways R81.10 (EOS),R81 (EOS),R80.40 (EOS)
  - Spark Firewalls R80.20.X (EOS), R81.10.X, R82.00.X
- 資料來源：
  1. checkpoint CVE-2026-50751
  2. CVE-2026-50751

2.3.11 Oracle針對旗下多款產品發布重大資安公告

CVE 編號	詳見官網附件
影響產品	詳見官網附件
解決辦法	根據官方網站釋出的解決方式進行修補： https://www.oracle.com/security-s/cspujun2026.html

- 內容說明：

  Oracle 近期釋出 115 年 6 月關鍵安全性修補程式更新公告，包含多個重大安全漏洞，請儘速確認並進行修補。(詳見附件說明)

- 影響平台：
  - 詳見官網附件
- 資料來源：
  1. Oracle Critical Security Patch Update Advisory - June 2026

2.3.12 Fortinet 防火牆等設備遭受憑證竊取攻擊，請儘速確認並修補

CVE 編號	無
影響產品	Fortinet 防火牆與 VPN 裝置
解決辦法	隱藏管理介面：盡速確認設備管理介面是否暴露於網際網路，並將管理介面從公開網際網路移除，僅允許受信任的 IP 或透過跳板機/VPN 方式存取。 全面重置設備密碼：立即更換所有 Fortinet 設備管理介面與 VPN 之管理者密碼。 啟用多因子驗證機制（MFA）：建議在所有遠端存取與管理員帳戶啟用多因素認證。 強制升級雜湊演算法：升級 FortiOS 後，要求所有管理員至少登入一次防火牆，系統會自動將密碼加密方式升級為更難被破解的 PBKDF2 演算法。

- 內容說明：

  研究人員發現有攻擊者針對 Fortinet 防火牆與 VPN 裝置等設備進行大規模憑證竊取攻擊，且疑似掌握相關設備之帳密資料，進而大規模破解相關設備防護措施。

  可運用下列查詢工具確認自身設備是否已遭揭露，並請盡速採取改善措施。

  工具連結：https://www.hudsonrock.com/fortinet

2.3.13 Cisco 旗下身分識別服務存在重大資安漏洞(CVE-2026-20181)

CVE 編號	CVE-2026-20181
影響產品	Cisco ISE、ISE-PIC
解決辦法	請更新至以下版本： Cisco ISE 和 Cisco ISE-PIC 3.3 Patch 11 Cisco ISE 和 Cisco ISE-PIC 3.4 Patch 6 Cisco ISE 和 Cisco ISE-PIC 3.5 Patch 4

- 內容說明：

  Cisco 旗下身分識別服務引擎(Identity Services Engine，ISE)是一款基於身分的安全管理平台，可從網路、使用者設備收集資訊，並在網路基礎設施中實施策略和制定監管決策。近日 Cisco 發布重大資安漏洞公告(CVE-2026-20181，CVSS：9.1)，此漏洞可能允許經過身分驗證的遠端攻擊者，在受影響設備的底層作業系統上執行任意命令。

  備註：若利用此漏洞，攻擊者必須擁有有效的管理員憑證。

- 影響平台：
  - Cisco ISE 和 Cisco ISE-PIC 3.3 (含)之前版本
  - Cisco ISE 和 Cisco ISE-PIC 3.4 版本
  - Cisco ISE 和 Cisco ISE-PIC 3.5 版本
- 資料來源：
  1. Cisco Identity Services Engine Remote Code Execution and Information Disclosure Vulnerabilities
  2. CVE-2026-20181

第 3 章、資安研討會及活動

- **資安研討會**

115年個人資料檔案安全維護計畫一對一線上健檢諮詢(限定資訊服務業者參與)	
活動時間	**2026-03-25 13:30 ~ 2026-07-30 14:30**
活動地點	**採預約制，線上Teams會議室**
活動網站	**https://www.tissa.org.tw/Course/Detail/5976**
活動概要	 **【費用】** 免費 報名截止： 2026-07-30 **【活動內容 / Event Deails】** 個資保護不只合規，專家一對一陪你實務到位！貴公司的個資安全維護計畫，經得起檢查嗎？小心受罰 2 萬元以上 200 萬元以下罰鍰！本活動由法律 + 資安專家團隊協助資服業者 1 on 1 線上諮詢。不僅協助快速找出關鍵漏洞，更提供最貼近實務面的改善建議作法！限 50 家資訊服務業者參與，立即搶先報名！

	*請在報名頁面【備註】欄位，留下三個您方便的日期，承辦人將收到您的資訊後，安排一對一線上健檢諮詢時段，謝謝！ **【主辦單位】財團法人資訊工業策進會** **【執行單位】中華民國資訊軟體服務商業同業公會** **【聯絡窗口】02-2553-3988#816 林專員** **security@tissa.org.tw**
115年資安事件應變工程師課程_健行科技大學（週五班）	
活動時間	**115/07/17(五)~115/08/14(五)**
活動地點	**健行科技大學商學院（桃園市中壢區健行路229號）C402教室**
活動網站	**http://eec.uch.edu.tw/web3/index3.asp?cid=318250**
活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】** 第一線保護系統並回應攻擊之系統管理員或其他安全人員，或是轉投入資安領域之 IT 人員、技術人員、系統維護人員及資訊管理人員等。 **【預備知識】** 需具備網路基礎知識(如網路設備、TCP/IP 及常見網路協定等)、作業系統基礎知識、資安防護概念(熟悉常見的資安防護機制如防火

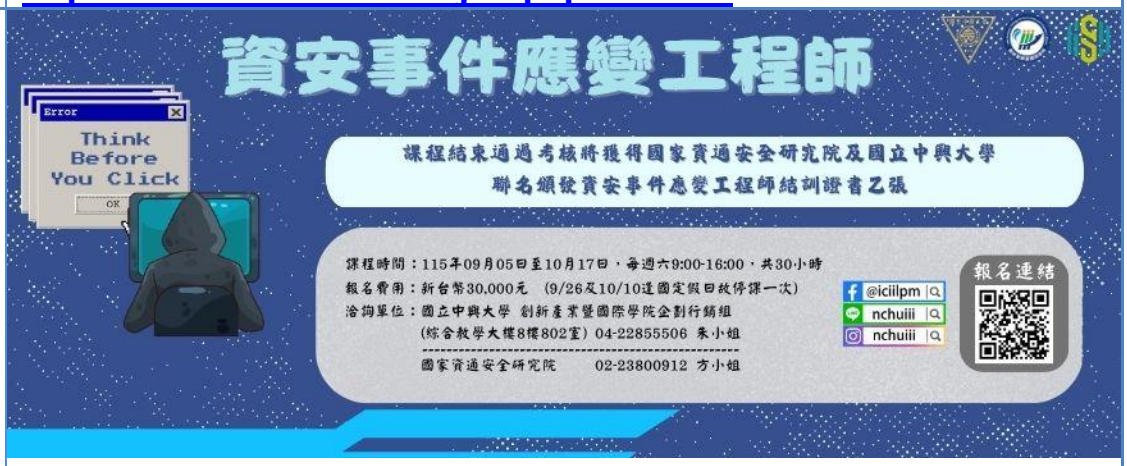
	牆、防毒軟體、入侵偵測系統等)，以及資訊安全管理基本概念(如風險評估)。 **【課程目標】** 了解資安事件的基本定義與範圍、資安事件的類型、資安事件應變流程說明資安事件的定義及分類，透過案例場景討論資安事件緊急應變的流程，並介紹 NIST SP 800-61 資安事件處理生命週期的 4 個階段細部內容，包括準備階段、偵測與分析階段、封鎖、根除與復原階段、事後處置階段。 **【師資介紹】蔡嘉志老師 / 健行科技大學資工系助理教授** **【主辦單位】國家資通安全研究院、健行科技大學**
115年資安事件應變工程師課程_健行科技大學（週六班）	
活動時間	**115/07/18(六)~115/08/15(六)**
活動地點	**健行科技大學商學院（桃園市中壢區健行路229號）C402教室**
活動網站	**http://eec.uch.edu.tw/web3/index3.asp?cid=318249**
活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】**

	第一線保護系統並回應攻擊之系統管理員或其他安全人員，或是轉投入資安領域之 IT 人員、技術人員、系統維護人員及資訊管理人員等。 **【預備知識】** 需具備網路基礎知識(如網路設備、TCP/IP 及常見網路協定等)、作業系統基礎知識、資安防護概念(熟悉常見的資安防護機制如防火牆、防毒軟體、入侵偵測系統等)，以及資訊安全管理基本概念(如風險評估)。 **【課程目標】** 了解資安事件的基本定義與範圍、資安事件的類型、資安事件應變流程說明資安事件的定義及分類，透過案例場景討論資安事件緊急應變的流程，並介紹 NIST SP 800-61 資安事件處理生命週期的 4 個階段細部內容，包括準備階段、偵測與分析階段、封鎖、根除與復原階段、事後處置階段。 **【師資介紹】蔡嘉志老師 / 健行科技大學資工系助理教授** **【主辦單位】國家資通安全研究院、健行科技大學**
115年資安事件應變工程師課程_朝陽科技大學（115001期）	
活動時間	**115/08/03(一)~115/08/07(五)**
活動地點	**朝陽科技大學推廣教育處中科分部（臺中市西屯區科園路21號）**
活動網站	**https://oce.cyut.edu.tw/course/n_course_detail.php?u=45264010e1a6708ea58bc84e71974cff**

活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】** 1.第一線保護/回應攻擊之系統管理員或其他安全人員。 2.轉投入資安領域之 IT 技術、系統維護或資訊管理人員。 3.擬投入資安教育之教師。 **【預備知識】** 資通安全概論、網路架構與部署安全。 **【課程目標】** 具備資安事件應變完整生命週期之基礎知識與各階段之操作技能。 **【師資介紹】許晉銘老師** **【主辦單位】國家資通安全研究院、朝陽科技大學**
115年資安事件應變工程師課程_逢甲大學	
活動時間	**115/8/29(六)~115/10/3(六)**
活動地點	**逢甲大學 校本部**
活動網站	**https://extension.fcu.edu.tw/#/course?Id=d350837b-becd-4e49-8506-86ef368ef29e**

活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】** 資訊技術從業人員、資安人員、資訊科系畢業等對資安有基本認知之人士。 **【預備知識】** 對網路架構與設定有基本認知與設定能力、能夠查詢正在執行的程序並判斷異常、知道防毒軟體與防火牆的基本原理等。 **【課程目標】** 1.建構標準化應變流程：訓練學員熟練掌握「準備、辨識、圍堵、根除、復原、經驗總結」六大階段，確保在壓力環境下仍能依循標準程序執行任務，避免應變失當造成二次傷害。 2.強化威脅偵測與情資研判：訓練學員解讀各類資安警報與日誌資訊，能快速辨識攻擊樣態（如 APT 攻擊、DDoS、勒索病毒），並結合威脅情資進行精準的風險評估。 3.精進圍堵與根除實戰技術：透過模擬實作，學習如何迅速隔離受感染主機、封鎖惡意連線，並徹底清除潛伏於系統內的後門程序，防止攻擊活動再次擴散。

	4.優化應變報告與經驗回饋：培養學員撰寫專業的「事後檢討報告（AAR）」，能針對應變過程提出具體的改善建議，協助組織優化防禦架構，化危機為轉機。 **【師資介紹】張舜賢、翁家鴻** **【主辦單位】國家資通安全研究院、逢甲大學**
115年資安事件應變工程師培訓班_崑山科技大學（平日班）	
活動時間	**115/08/31(一)~115/09/04(五)**
活動地點	**崑山科技大學 圖書資訊館8樓**
活動網站	**https://cee.ksu.edu.tw/CourseInfo.aspx?id=3614**
活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】** 對於本課程有興趣者皆可報名。 **【預備知識】** 建議具備資通訊安全的概念。 **【課程目標】** 使學員了解資安事件應變處理之完整流程，並能利用課程學習內容，於資安事件之事前、事中、事後階段進行有效之應處，從而降低組織的資安風險並減少造成的損失。 **【師資介紹】鄭郁翰老師 / 崑山科技大學** **【主辦單位】國家資通安全研究院、崑山科技大學**

115年資安事件應變工程師課程_國立中興大學	
活動時間	115/9/5(六)~115/10/17(六)
活動地點	國立中興大學
活動網站	https://www.siileec.com/subject.php?sn=6326
活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】** 第一線保護系統並回應攻擊之系統管理員或其他安全人員、轉投入資安領域之 IT 技術人員、系統維護人員及資訊管理人員、具資訊相關背景，對於資安事件應變流程有興趣者。 **【預備知識】** 課程對象不限政府機關或是業界人員，對於本課程有興趣之人員皆可受訓。惟課程對於受訓學員有先備知識的建議，希望參加課程的學員至少有資通訊安全的概念。 **【課程目標】** 培訓學員具備資安事件應變完整生命週期之基礎知識與各階段之操作技能，使學員了解資安事件應變處理之完整流程，並能於資安事件之事前、事中、事後階段進行有效之應處，從而降低組織的資安風險並減少造成的損失。

	【師資介紹】吳啟文、徐振煒、李慈偉、許炳昆 【主辦單位】國家資通安全研究院、國立中興大學
115年資安事件應變工程師課程_朝陽科技大學（115002期）	
活動時間	115/10/19(一)~115/10/23(五)
活動地點	朝陽科技大學推廣教育處中科分部（臺中市西屯區科園路21號）
活動網站	https://oce.cyut.edu.tw/course/n_course_detail.php?u=acc65ac9182a9a9db8c6b10027ff1621
活動概要	 【費用】 依各訓練機構收費標準，請參閱報名連結。 【招生對象】 1.第一線保護/回應攻擊之系統管理員或其他安全人員。 2.轉投入資安領域之 IT 技術、系統維護或資訊管理人員。 3.擬投入資安教育之教師。 【預備知識】 資通安全概論、網路架構與部署安全。 【課程目標】 具備資安事件應變完整生命週期之基礎知識與各階段之操作技能。 【師資介紹】許晉銘老師 【主辦單位】國家資通安全研究院、朝陽科技大學

115年滲透測試工程師課程_國立中興大學	
活動時間	**115/11/7(六)~115/12/5(六)**
活動地點	**國立中興大學**
活動網站	**https://www.siileec.com/subject.php?sn=6327**
活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】** 系統管理或其他網路安全管理人員、安全事件回應處理相關管理人員、資安技術服務/弱點檢測人員。 **【預備知識】** 基礎資訊技術與資安概、基礎網路安全與 Web、技術分析與邏輯推論能力、風險管理與法律倫理意識。 **【課程目標】** 訓練具備識別資訊系統中的弱點及漏洞，執行漏洞評估、風險分級與管理，提出可行且有效的補救與強化建議報告。 **【師資介紹】徐振煒、李慈偉、許炳昆** **【主辦單位】國家資通安全研究院、國立中興大學**

第 4 章、TVN 漏洞公告

TWCERT/CC 本月份發布之CVSS 3.1分數為8.8以上之漏洞資訊如下表：

基點資訊｜CelloOS - Improper Access Control	
TVN / CVE ID	TVN-202606002 / CVE-2026-12059
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	CelloOS 4.8.0 Build 20260316(不含)以前版本
問題描述	基點資訊開發之CelloOS之SSH服務存在Improper Access Control漏洞，已通過身分鑑別之遠端攻擊者可繞過原本的指令限制機制，進而執行未被授權的作業系統指令。
解決方法	原廠已於2026/3/18進行線上修補。若因離線、隔離或其他原因無法接收線上修補的系統，應手動更新至2026/3/18當日或之後發布的已修補版本。
公開日期	2026-06-12
相關連結	https://www.twcert.org.tw/tw/cp-132-10966-3258e-1.html
IEI 威強電工業電腦｜iRM-IEI Remote Management - Hardcoded Credentials	
TVN / CVE ID	TVN-202606005 / CVE-2026-11849
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	iRM-TSi410X v1.4.19(不含)以前版本
問題描述	【CVE-2026-11849(Hardcoded Credentials)】 未經身分鑑別之遠端攻擊者可利用hard-coded之帳號通行碼取得資料庫最高權限。
解決方法	更新至 iRM TSi410X v1.4.19(含)以後版本

公開日期	2026-06-12
相關連結	**https://www.twcert.org.tw/tw/cp-132-10971-ac61f-1.html**
研華科技｜Hospital Queuing Management - Hardcoded Credentials	
TVN / CVE ID	TVN-202606007 / CVE-2026-14162
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	Hospital Queuing Management(HQM) ISO 1.2.13(不含)以前版本
問題描述	【CVE-2026-14162(Missing Authentication)】 未經身分鑑別之遠端攻擊者可利用API取得機敏資訊或新增網站管理員帳號。
解決方法	請更新HQM ISO至 1.2.13(含)以後版本或更新QueueHttp.dll至1.2.12.7(含)以後版本
公開日期	2026-06-30
相關連結	**https://www.twcert.org.tw/tw/cp-132-11011-999eb-1.html**

編輯：**TWCERT/CC 團隊**

發行單位：**台灣電腦網路危機處理暨協調中心**
(Taiwan Computer Emergency Response Team / Coordination Center)

出刊日期：**2026年6月30日**

電子郵件：**CERT_Service@cert.org.tw**

官網：**https://twcert.org.tw/**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc/**

Instagram：**https://www.instagram.com/twcertcc/**