TWCERT/CC 資安情資電子報

2025 年 9 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

第 1 章、封面故事

解密「長線佈局」與跨領域攻擊：CrowdStrike 深入解析 2025 駭客戰術演進

CrowdStrike 最新威脅報告指出，在2024年7月1日至2025年6月30日期間，互動式入侵（interactive intrusion）事件年增27%，此類攻擊不同於以往的自動化入侵，駭客會在取得權限後，主動與受害電腦環境互動，蒐集資訊並依據情境客製化攻擊策略。其中，超過八成的案例涉及無檔案惡意軟體（fileless malware），顯示傳統依賴檔案檢測的防禦方式已面臨挑戰。

雲端與語音詐騙成為新焦點

報告同時揭示，中國針對雲端的攻擊年增40%，突顯雲端服務仍是國家級攻擊者的主要戰場。此外，語音詐騙在2024下半年成長率高達442%，並於2025上半年已超越2024全年數量，顯示AI技術的普及正加速此類詐騙的規模與影響。

國家級攻擊與產業目標

科技業至今已連續8年成為遭攻擊最多的產業，主要來自網路犯罪活動，而APT攻擊則鎖定電信與政府單位。其中，俄羅斯行為者以PRIMITIVE BEAR 與 VENOMOUS BEAR 為主，攻擊目的與俄烏戰爭相關；中國行為者則將電信產業視為高價值目標，藉此取得用戶資料、滲透下游客戶，相關攻擊在過去一年成長130%。

製造與零售業的高風險處境

製造與零售產業在過去一年也成為攻擊熱點。CURLY SPIDER 駭客組織頻繁施以勒索軟體並結合語音詐騙，利用這些產業對營運不中斷的高度依賴迫使受害者快速付款。如製造業無法承擔生產中斷的損失；零售業在購物旺季期間若資料外洩或系統停擺，將損失客戶與營收。此外，其產業具有龐大預算、複雜且可能過時的 IT 架構，使得這些產業持續吸引網路犯罪集團的目光。

生成式AI成為攻擊加速器

CrowdStrike 指出，攻擊者正積極將生成式 AI（GenAI）整合於作戰流程，並非取代而是強化原有戰術與技術。APT 組織透過 GenAI 加快滲透與作業效率，而一般網路犯罪者則利用 GenAI 自動化腳本撰寫與問題排解。其影響主要體現在以下三個面向：

1. 撰寫更自然和符合應對情境的釣魚信件，並持續針對歐盟和美國發動釣魚攻擊，且能進行身分偽造
2. 更容易生成虛假影片、音訊和圖片，並冒充知名人物（deepfake）
3. 降低資安攻擊門檻，加速提高惡意攻擊程式生成

實際案例與新興威脅

北韓 FAMOUS CHOLLIMA 組織便是典型案例。他們透過 GenAI 偽造求職者身份、製作 deepfake 視訊，並藉由 LLM 增強英文對答與技術能力，以成功取得遠端工程師職位。過去一年已觀察到超過 320 起相關資安事件。此外，2025 年 4 月，駭客組織更將攻擊目標轉向 AI 開發工具 Langflow AI（CVE-2025-3248），顯示 AI 平台本身也成為潛在的攻擊面。

面對上述威脅，CrowdStrike提供以下防禦建議：

1. 企業應加強對應徵者的身分驗證，例如透過背景調查及查證其線上職涯紀錄，以避免遭遇假身分風險
2. 導入即時deepfake 偵測技術，應用於視訊面試與錄音評估中，辨識虛假影音資料
3. 加強遠端存取控管，防範位置偽裝與端點繞過，保護企業資源不受濫用
4. 全面檢查USB及周邊裝置，且驗證外接設備安全性，阻斷可能載入的遠端控制工具
5. 監控使用者的通訊與操作行為，藉由檢測異常翻譯與帳號同步操作等情形，判斷是否存在AI操控的可能
6. 針對招募與IT團隊設計AI滲透識別訓練課程，強化識別與應對

能力

報告總結指出，生成式AI不會單方面完全傾向攻擊方或防禦方，真正的差異在於使用者的技術能力，唯有同步強化技術偵測、治理政策及人員訓練，才能在不斷演進的攻防環境中維持韌性。

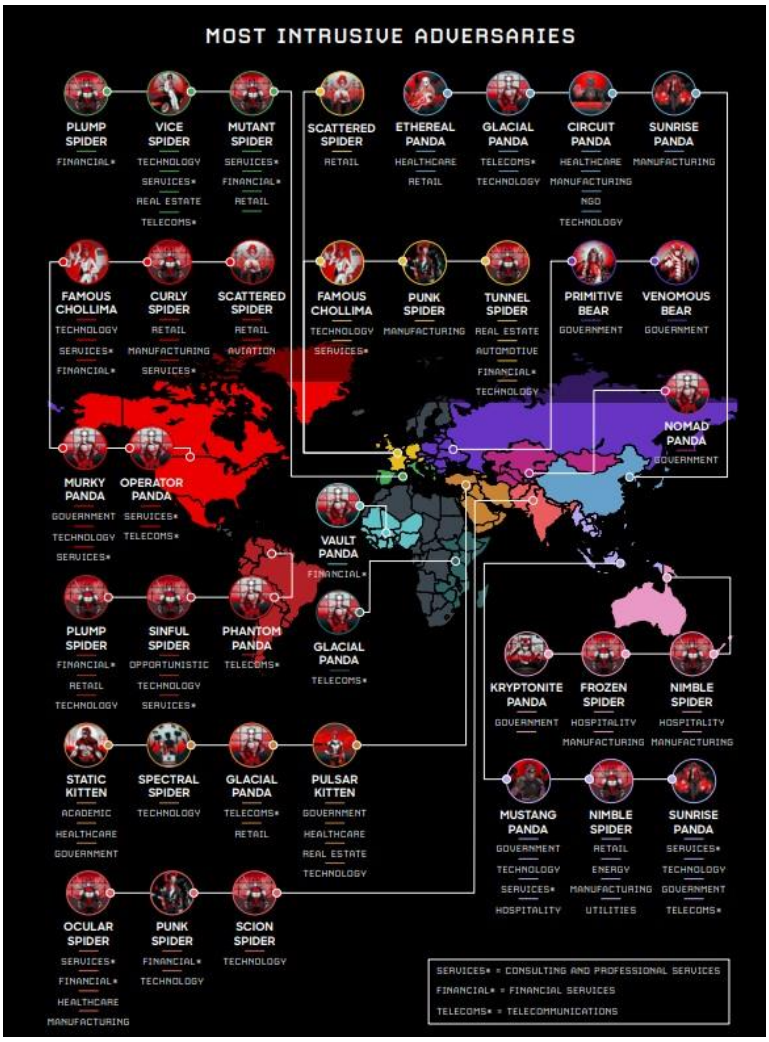

圖1：過去一年活躍的APT組織。圖片來源：CrowdStrike

CrowdStrike對威脅組織的定義與命名遵循特定規則，如下表 1 所示。例如，代表中國的高階持續性威脅（APT）組織名稱通常會包含「Panda」字樣，舉例來說，「Mustang Panda」便是此類命名規則的典

型代表。

名稱（**Adversary**）	國家 / 類別
BEAR	Russia
BUFFALO	Vietnam
CHOLLIMA	DPRK (North Korea)
CRANE	ROK (Republic of Korea)
HAWK	Syria
JACKAL	Hacktivist
KITTEN	Iran
LEOPARD	Pakistan
LYNX	Georgia
OCELOT	Colombia
PANDA	People's Republic of China
SAIGA	Kazakhstan
SPHINX	Egypt
SPIDER	eCrime
TIGER	India
WOLF	Türkiye

表1：CrowdStrike命名APT威脅組織的規則。由TWCERT/CC整理

Threat Actor	Country	Target Industries
SCATTERED PANDA	China	Retail
ETHEREAL PANDA	China	Healthcare, Retail
GLACIAL PANDA	China	Telecoms*, Technology, Retail
CIRCUIT PANDA	China	Healthcare, Manufacturing, NGO, Technology
SUNRISE PANDA	China	Manufacturing, Services*, Technology, Government, Telecoms*
MURKY PANDA	China	Government, Services*, Technology, Telecoms*
OPERATOR PANDA	China	Services*, Technology, Telecoms*
VAULT PANDA	China	Financial*
NOMAD PANDA	China	Government
PHANTOM PANDA	China	Telecoms*
SCATTERED PANDA	China	Retail
ETHEREAL PANDA	China	Healthcare, Retail
GLACIAL PANDA	China	Telecoms*, Technology, Retail

CIRCUIT PANDA	China	Healthcare, Manufacturing, NGO, Technology
SUNRISE PANDA	China	Manufacturing, Services*, Technology, Government, Telecoms*
KRYPTONITE PANDA	China	Government
MUSTANG PANDA	China	Government, Technology, Services*, Hospitality
PRIMITIVE BEAR	Russia	Government
VENOMOUS BEAR	Russia	Government
FAMOUS CHOLLIMA	North Korea (DPRK)	Technology, Services*, Financial*
PLUMP SPIDER	eCrime / Cybercriminal	Financial*, Retail, Technology
VICE SPIDER	eCrime / Cybercriminal	Technology, Services*, Real Estate, Telecoms*
MUTANT SPIDER	eCrime / Cybercriminal	Services*, Financial*, Retail
SCATTERED SPIDER	eCrime / Cybercriminal	Retail, Aviation
CURLY SPIDER	eCrime / Cybercriminal	Retail, Manufacturing, Services
TUNNEL SPIDER	eCrime / Cybercriminal	Real Estate, Automotive, Financial*, Technology
PUNK SPIDER	eCrime / Cybercriminal	Manufacturing, Financial*, Technology
SINFUL SPIDER	eCrime / Cybercriminal	Opportunistic, Technology, Services*
FROZEN SPIDER	eCrime / Cybercriminal	Hospitality, Manufacturing
NIMBLE SPIDER	eCrime / Cybercriminal	Hospitality, Manufacturing, Retail, Energy, Government, Utilities
STATIC KITTEN	Iran	Academic, Healthcare, Government
PULSAR KITTEN	Iran	Government, Healthcare, Real Estate, Technology

表2：CrowdStrike整理報告期間活躍APT組織。由TWCERT/CC整理

- 相關連結

1. CROWDSTRIKE：2025 THREAT HUNTING REPORT

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 駭客組織疑似聯手，資安威脅再升級

近期社群平台與威脅情資顯示，一個自稱由多個駭客組織所組成的聯盟「Scattered LapSus Hunters」開始備受矚目。雖然目前該聯盟尚未提出具體技術證據，證實成功入侵某國際雲端與網路服務供應商的資料庫，該企業亦未發現新增漏洞或入侵跡象，但影響力仍不容忽視。今年8月該企業曾證實其第三方合作廠商遭到另一個駭客組織「ShinyHunters」攻擊，造成部分資料外洩，值得注意的是，資安事件發生於第三方系統，非該企業的核心基礎架構，凸顯第三方供應鏈安全管理的重要性。

根據現有情資分析，「Scattered LapSus Hunters」疑似由三個知名駭客組織組成。這包括以複雜社交工程手法聞名的 「Scattered Spider」、

針對大型科技公司發動攻擊的「LapSus」，以及長期活躍於暗網，從事大規模資料外洩的「ShinyHunters」。若此聯盟確實成立，將代表不同攻擊手法和資源的整合，可能使網路威脅進一步升級，對企業資安防護帶來更大挑戰。

三個駭客組織各自採用不同且具特色的攻擊手法：

Scattered Spider 以先進的社交工程著稱，目標多為金融、零售、航空及供應鏈關鍵產業。該組織常利用冒充IT支援人員的手段，透過語音釣魚(Vishing)、SIM卡交換(SIM-swapping)、多因子認證疲勞(MFA bombing)等攻擊手法繞過多因子認證，竊取內部憑證並進行橫向移動，各國執法與資安機構已發布聯合諮詢與防範建議。

Lapsus（亦以 Microsoft 代號 DEV-0537）以鎖定大型科技或供應商後利用內部憑證與遠端桌面工具取得敏感資料、再以公開威脅或直接上傳暗網勒索聞名。該群組手法看似「不一定靠高階零日」，但靠持續社交工程、內部協助者或竊取管理憑證來達成破壞與外洩，並在公開平台（如 Telegram）散布被盜資料以施壓。其攻擊手法與影響力曾引起政府專門報告與檢討。

ShinyHunters 自 2020 年起多次公佈大量資料外洩，受害範圍包括電商、雲端服務及應用程式使用者資料。該組織透過社交工程攻擊手法與利用未修補的系統漏洞進行入侵，並迅速整理竊取的資料，隨即在暗網販售或公開外洩，形成持續且具高影響力的資料洩漏事件。

在觀察的三個駭客組織中，不難發現社交工程已成為其主要且常用的入侵手段，通常包括釣魚郵件、SIM swapping 與內部帳號收買等技術，面對駭客組織可能聯手帶來的升級威脅，組織不僅需強化既有的技術防護手段，更應提升員工的資安意識，加強防範社交工程攻擊的風險。同

時，應全面檢視供應鏈及第三方合作夥伴的資安措施，避免成為駭客的攻擊入口。此外，企業應建立跨部門協同的資安應變計畫，確保在面對大規模資料外洩或勒索攻擊時，能快速偵測、通報及回應，從而提升組織面對多個駭客組織聯合攻擊時的韌性與抵禦能力。

- 相關連結
  1. Hackers Reportedly Demand Google Fire Two Employees, Threaten Data
  2. How ShinyHunters Breached Google, Adidas, Louis Vuitton and More in Ongoing Salesforce Attack Campai
  3. CISA - Scattered Spider
  4. DEV-0537 criminal actor targeting organizations for data exfiltration and destruction
  5. Researchers firm up ShinyHunters, Scattered Spider link

2.2 新興應用資安

2.2.1 LLM防線全面失守？資安研究員用ChatGPT模擬攻擊竟生成數千惡意樣本

Palo Alto Networks 近期研究報告，公開大型語言模型（LLM）使非程式設計背景的使用者能在數小時內自動產生大量具有攻擊能力的惡意程式碼樣本，如資料竊取器、勒索軟體等，甚至可能產生尚未出現新變種。研究也指出，現有的防護機制（如：prompt 過濾）容易被「jailbreaking」技巧輕易繞過，資安風險大幅提升。

為了驗證此項資安威脅，Palo Alto Networks的研究團隊設計一套自動化生成惡意程式的流程（如圖1所示），流程包括：

1. 提供特定惡意軟體的資安報告作為輸入資料
2. 將報告內容載入並送入LLM作為 prompt 指令來源
3. 透過多次修正與人機反饋迴圈，不斷調整提示以引導模型生成惡

意程式碼

4. 儲存程式與對話紀錄，並進行功能驗證

研究結果顯示，該流程能在短時間內自動化生成數千個具備實際攻擊能力的惡意程式樣本，資安專家警告，「這已不僅是技術門檻的降低，更是進入『量產級』的攻擊時代」。

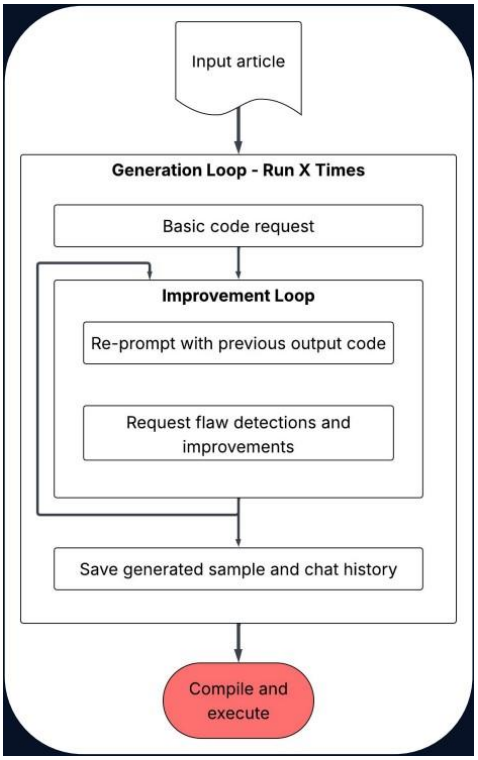

圖1：自動化生成惡意程式的系統。圖片來源 Palo Alto Networks

Palo Alto Networks研究團隊指出，儘管惡意程式樣態不斷演變，只要涉及檔案加密、資料竊取或遠端連線等惡意行為，仍可透過行為式防禦機制進行攔截，顯示傳統依賴特徵比對的防禦模式已難以有效因應新型威脅，資安團隊必須重新檢視並調整整體防禦策略。

為協助組織更有效抵禦未知威脅，該團隊提出「預測式威脅情報循環（Predictive Threat Intelligence Cycle）」，如圖2所示，其核心理念包

含：

1. 主動假設未來可能的攻擊手法
2. 自行生成或變種威脅樣本、模擬多元攻擊情境
3. 測試並驗證現有防護機制能否抵禦假想威脅，在攻擊發生前即時修補防禦缺口

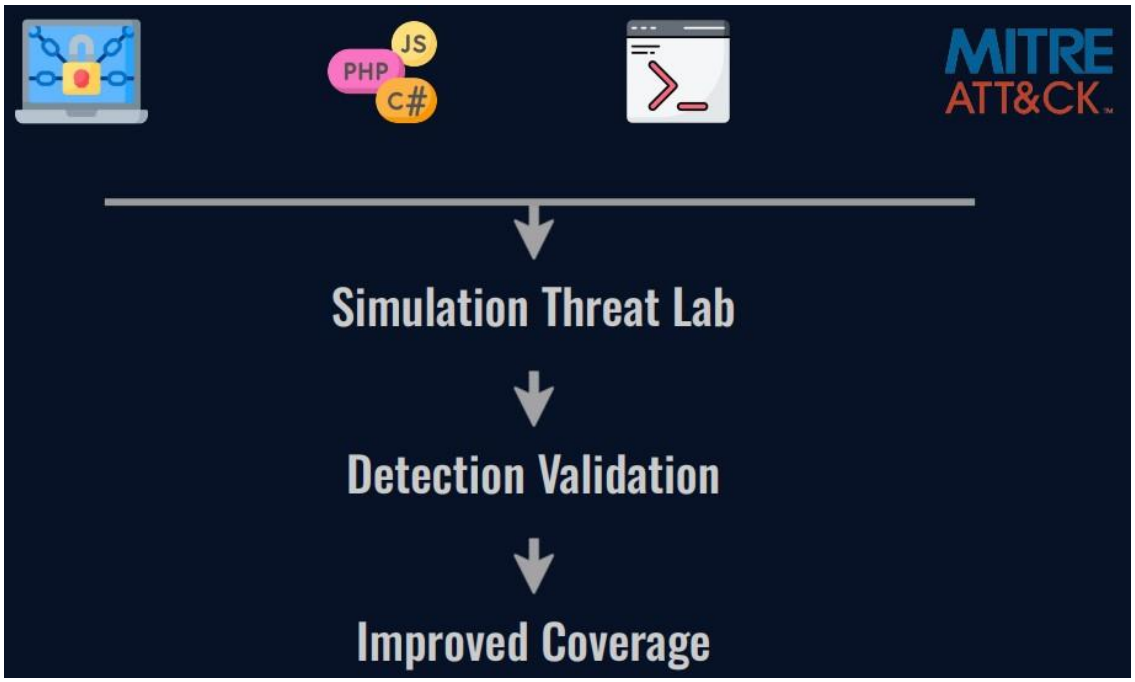

圖2：威脅情報新的轉型樣貌。圖片來源： Palo Alto Networks

隨著生成式AI的迅速發展，世界正式步入「惡意軟體零門檻生成」時代，這不僅改變攻擊者的面貌，更迫使資安團隊重新思考與定義「防禦」的核心價值。在這場全新的攻防競賽中，唯有主動預測威脅並模擬潛在攻擊，才能在攻擊發生之前築起有效防線。

- 相關連結
  1. Rem Dudas & Bar Matalon: Draw Me a Virus: Proact Threat Intelligence in the Era of AI-Gen Malware

2.3 軟硬體漏洞資訊

2.3.1 Sophos旗下AP6系列無線存取點存在重大資安漏洞

CVE 編號	CVE-2025-10159
影響產品	Sophos AP6 系列無線存取點
解決辦法	將 AP6 系列無線存取點韌體版本更新至 1.7.2563(含)之後版本

- 內容說明：

  Sophos 針對旗下 AP6 系列無線存取點發布重大資安公告(CVE-2025-10159，CVSS：9.8)，此為身分驗證繞過漏洞，允許攻擊者存取無線存取點的管理 IP 位址，從而取得管理員權限。

  備註：採用預設自動更新政策的用戶無需額外動作；若已停用自動更新，請手動升級以修正本次安全漏洞。

- 影響平台：
  - AP6 系列無線存取點韌體版本 1.7.2563(不含)之前版本
- 資料來源：
  1. Resolved Authentication Bypass Vulnerability in Sophos AP6 Series Wireless Access Points Firmware
  2. CVE-2025-10159

2.3.2 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2025-42944,CVE-2025-42922,CVE-2025-42958,CVE-2025-42933
影響產品	SAP NetWeaver、NetWeaver AS Java、Business One
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/september-2025.html

- 內容說明：

【CVE-2025-42944，CVSS：10.0】

SAP NetWeaver 存在反序列化漏洞。未經驗證的攻擊者可透過 RMI-P4 模組，向對外開放的連接埠傳送惡意負載，進而執行任意作業系統命令，對應用程式的機密性、完整性及可用性構成潛在威脅。

【CVE-2025-42922，CVSS：9.9】

SAP NetWeaver AS Java 存在允許經過管理身分驗證的攻擊者上傳任意檔案的漏洞，可能導致系統的機密性、完整性和可用性造成破壞。

【CVE-2025-42958，CVSS：9.1】

IBM i-series 的 SAP NetWeaver 應用程式缺少身分驗證檢查，允許高權限的未經授權使用者讀取、修改或刪除敏感資料，並進一步存取管理功能或以特權權限操作，對應用程式的機密性、完整性與可用性構成重大風險。

【CVE-2025-42933，CVSS：8.8】

當用戶透過 SAP Business One 原生用戶端登入時，由於 SLD 後端服務未對部分 API 強制使用適當的加密機制，導致敏感憑證可能在 HTTP 回應主體中外洩，進而嚴重影響應用程式的機密性、完整性與可用性。

- 影響平台：
  - SAP Netweaver (RMI-P4) SERVERCORE 7.50
  - SAP NetWeaver AS Java J2EE-APPS 7.50
  - SAP NetWeaver KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54
  - SAP Business One (SLD) B1_ON_HANA 10.0, SAP-M-BO 10.0
- 資料來源：
  1. SAP Security Patch Day - September 2025
  2. CVE-2025-42944
  3. CVE-2025-42922
  4. CVE-2025-42958
  5. CVE-2025-42933

2.3.3 Ivanti 旗下Connect Secure、Policy Secure、ZTA Gateways和 Neurons for Secure Access存在多個重大資安漏洞

CVE 編號	CVE-2025-55141,CVE-2025-55142,CVE-2025-55145,CVE-2025-55147
影響產品	Ivanti Connect Secure、Policy Secure、ZTA Gateway、Neurons for Secure Access
解決辦法	請更新至以下版本： Ivanti Connect Secure 22.7R2.9 Ivanti Connect Secure 22.8R2 Ivanti Policy Secure 22.7R1.6 Ivanti ZTA Gateway 2.8R2.3-723 Ivanti Neurons for Secure Access 22.8R1.4

- 內容說明：

【CVE-2025-55141，CVSS：8.8】

此漏洞在受影響設備中缺乏授權機制，允許經過身分驗證且具有唯讀管理者權限的攻擊者修改與身分驗證相關的設定。

【CVE-2025-55142，CVSS：8.8】

此漏洞在受影響設備中缺乏授權機制，允許經過身分驗證且具有唯讀管理者權限的攻擊者修改與身分驗證相關的設定。

【CVE-2025-55145，CVSS：8.9】

此漏洞在受影響設備中缺乏授權機制，允許經過身分驗證的遠端攻擊者，劫持現有的 HTML5 連線。

【CVE-2025-55147，CVSS：8.8】

此漏洞在受影響設備中存在 CSRF 漏洞，允許經過身分驗證的遠端攻擊者，以受害者用戶的身分執行敏感性操作。

- 影響平台：
  - Ivanti Connect Secure 22.7R2.8 (含)之前版本
  - Ivanti Policy Secure 22.7R1.5 (含)之前版本
  - Ivanti ZTA Gateway 2.8R2.2 (含)之前版本
  - Ivanti Neurons for Secure Access 22.8R1.3 (含)之前版本
- 資料來源：
  1. September Security Advisory Ivanti
  2. CVE-2025-55141
  3. CVE-2025-55142
  4. CVE-2025-55145
  5. CVE-2025-55147

2.3.4 Cisco IOS XE存在高風險資安漏洞

CVE 編號	CVE-2025-20334
影響產品	Cisco IOS XE
解決辦法	請參考官方說明進行更新： https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL

- 內容說明：

  Cisco 發布重大資安漏洞公告(CVE-2025-20334，CVSS：8.8)，此漏洞存在於 Cisco IOS XE 的 HTTP API 子系統，因輸入驗證不足，允許具有管理者權限的攻擊者，可透過精心設計的 API 請求向受影響的系統進行身分驗證；或未經身分驗證的遠端攻擊者誘使具有管理者權限的合法使用者點擊精心設計的連結以觸發漏洞。當漏洞成功利用後，攻擊者可能以 root 身分在受影響系統上執行任意命令。

- 影響平台：
  - Cisco IOS XE 系統已啟用 HTTP 伺服器功能，建議至官方網站查詢版本以確定是否受此漏洞影響。https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL#fs

- 資料來源：
  1. Cisco IOS XE Software HTTP API Command Injection Vulnerability
  2. CVE-2025-20334
  3. CVE-2025-20334

2.3.5 Cisco 旗下防火牆系統存在二個重大資安漏洞

CVE 編號	CVE-2025-20333,CVE-2025-20363
影響產品	Cisco ASA、FTD
解決辦法	根據官方網站釋出解決方式進行修補： https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB

- 內容說明：

【CVE-2025-20333】

Cisco 安全防火牆自適應安全設備(ASA)和 Cisco 安全防火牆威脅防禦(FTD)的 VPN Web 伺服器中存在重大資安漏洞(CVE-2025-20333，CVSS：9.9)。此漏洞源自伺服器對使用者輸入 HTTP(S)請求驗證不當，持有有效 VPN 使用者憑證的攻擊者，可藉由精心設計的 HTTP 請求，允許經身分驗證的遠端攻擊者以 root 身分在受影響設備執行任意程式碼。

【CVE-2025-20363】

Cisco 安全防火牆自適應安全設備(ASA)、Cisco 安全防火牆威脅防禦(FTD)軟體、Cisco IOS 軟體、Cisco IOS XE 軟體和 Cisco IOS XR 軟體的 Web 服務存在重大資安漏洞(CVE-2025-20363，CVSS：9.0)。此漏洞源於 HTTP 請求對使用者輸入驗證不當，攻擊者可向受影響設備的 Web 服務發送精心設計的 HTTP 請求，以 root 身分執行任意程式碼，從而導致受影響裝置中斷服務。

- 影響平台：
  - 建議至官方網站查詢版本以確定是否受此漏洞影響。
    https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
  - 若 ASA 和 FTD 具有以下列出一個或多個設定，建議至官方網站查詢版本以確定是否受此漏洞影響。
    1. IOS 軟體啟用遠端存取 SSL VPN 功能
    2. IOS XE 軟體啟用遠端存取 SSL VPN 功能
    3. IOS XR 軟體(32 位元)啟用 Cisco ASR 9001 路由器有 HTTP 伺服器
    https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O
- 資料來源：
  1. Cisco Secure Firewall ASA and FTD Software VPN Web Server Remote Code Execution Vulnerability
  2. CVE-2025-20333
  3. Cisco Secure Firewall ASA, FTD, IOS Software,IOS XE Software, and Cisco IOS XR Software Web Service
  4. CVE-2025-20363

第 3 章、資安研討會及活動

- **資安研討會**

【資安競賽】資安技能金盾獎競賽	
活動時間	**2025/10/18 、 2026/01/09**
活動地點	**致理科技大學、臺中科技大學、文藻外語大學、臺北文創大樓**
活動網站	**https://csc.nics.nat.gov.tw/shield.aspx**
活動概要	**【費用】** 免費 報名截止： 2025/10/03 17:00 **【活動內容 / Event Deails】** 加強學生資安實務技能，培育成在資安領域中獨立思考和行動的專業人才，拓展學生在資安領域的能力。以實務與時事題型，運用理論及知識基礎，在模擬真實情境中學習，應對當前資安領域的挑戰和問題，了解資安的發展與趨勢，進而提升學子解決問題能力和實戰經驗。 **【指導單位】數位發展部、教育部** **【主辦單位】數位發展部資通安全署** **【承辦單位】國家資通安全研究院** **【聯絡窗口】02-2528-8278 轉 23、24 謝先生、曾小姐** **cscservice@nics.nat.gov.tw**
【數位產業署】關鍵基礎設施-電力系統資安系列課程I(沙崙 X 成大太陽能系統)	
活動時間	**2025/10/13 08:30 ~ 16:00**
活動地點	**臺南市東區大學路1號**

活動網站	https://ievents.iii.org.tw/EventS.aspx?t=0&id=2989
活動概要	 **【費用】** 免費 報名截止： 2025/10/07 **【課程目標 / Event Deails】** 1. 讓學員熟悉太陽能系統架構、通訊協定及資安防護重點。 2. 掌握 Modbus 封包分析、封包逆向與漏洞探討方法。 3. 學會運用滲透測試腳本與防禦策略，模擬真實攻擊與防禦情境。 4. 建立以系統模型進行資安演練的能力，提升工控系統防護水準。 **【主辦單位】數位部數位產業署** **【主辦單位】財團法人資訊工業策進會** **【聯絡窗口】06-3032260#145 陳小姐** yuxuanchen@iii.org.tw
【數位產業署】關鍵基礎設施-電力系統資安系列課程II(沙崙 X 成大饋線自動化系統)	
活動時間	**2025/10/14 08:30 ~ 16:00**
活動地點	**臺南市東區大學路1號**
活動網站	https://ievents.iii.org.tw/EventS.aspx?t=0&id=2990

活動概要	 **【費用】** 免費 報名截止： 2025/10/07 **【課程目標 / Event Deails】** 1. 熟悉饋線自動化系統架構、通訊協定及資安防護重點。 2. 掌握 Modbus 封包分析、封包逆向與漏洞分析技術。 3. 學會使用滲透測試腳本進行實務攻防演練。 4. 能根據 MITRE ATT&CK for ICS 框架規劃與實施資安防禦策略。 5. 提升在真實電力系統場域中應對與防範資安威脅的能力。 **【主辦單位】數位部數位產業署** **【協辦單位】財團法人資訊工業策進會** **【聯絡窗口】06-3032260#145 陳小姐** **yuxuanchen@iii.org.tw**

【數位產業署】 關鍵基礎設施-電力系統資安系列課程III(電驛系統工控資安)	
活動時間	**2025/10/27 08:30 ~ 16:00**
活動地點	**臺南市東區大學路1號**
活動網站	**https://ievents.iii.org.tw/EventS.aspx?t=0&id=2991**

活動概要	 **【費用】** 免費 報名截止： 2025/10/07 **【課程目標 / Event Deails】** 1. 了解電驛系統測台的架構、部署方式及運作原理。 2. 學習 MMS 封包的側錄、解析與逆向工程技術。 3. 掌握工控環境下漏洞分析與攻擊鏈設計思維。 4. 能夠使用滲透測試腳本，實作未授權指令與偽造訊息等攻擊模擬。 5. 熟悉 MITRE ATT&CK for ICS 框架，並能據此規劃資安防禦策略。 6. 提升在真實電力系統場域中識別、分析與應對資安威脅的能力。 **【主辦單位】數位部數位產業署** **【協辦單位】財團法人資訊工業策進會** **【聯絡窗口】06-3032260#145 陳小姐** **yuxuanchen@iii.org.tw**

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：

全景軟體｜時戳伺服器(TSA) - Missing Authentication	
TVN / CVE ID	TVN-202508005 / CVE-2025-8861
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	時戳伺服器(TSA)，2025/2/6之前購買才會受到影響
問題描述	全景軟體開發之時戳伺服器(TSA)存在Missing Authentication漏洞，允許未經身分鑑別之遠端攻擊者利用開發者工具讀取、修改及刪除資料庫內容。
解決方法	聯繫廠商確認是否完成修補
公開日期	2025-08-29
相關連結	https://www.twcert.org.tw/tw/cp-132-10360-012e7-1.html
全景軟體｜醫療病歷文件掃描倉儲系統 - Hard-coded Credentials	
TVN / CVE ID	TVN-202508006 / CVE-2025-8857
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	醫療病歷文件掃描倉儲系統 2.4.23.2131 (含)之前版本，1.5.x.x與2.0.x.x版本除外
問題描述	全景軟體開發之醫療病歷文件掃描倉儲系統存在Hard-coded Credentials漏洞，未經身分鑑別之遠端攻擊者可利用寫入於原始碼中的管理帳號與通行碼登入系統。
解決方法	更新至2.4.23.2131(不含)以後版本
公開日期	2025-08-29

相關連結	https://www.twcert.org.tw/tw/cp-132-10362-c6021-1.html
永恒數位通訊科技｜網路監控伺服器 - 存在2個漏洞	
TVN / CVE ID	TVN-202509001 / CVE-2025-10264, CVE-2025-10265
CVSS	CVE-2025-10264： 10 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H CVE-2025-10265： 8.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	受影響NVR系列型號： DS-1200 DS-2100 Pro DS-2100 Pro+ DS-2100 UHD DS-2200 UHD DS-2200 UHD+ DS-4200 Pro DS-4200 Pro+ DS-4200 UHD DS-4200 UHD+ DS-4100-RM DS-4200-RM Pro+ DS-4200-RM UHD DS-8x00-RM Pro+ DS-8x00-SRM Pro+ DS-8x00-RM UHD DS-16x00-RM Pro+ DS-16x00-RM UHD 受影響Firmware版本： x.x.x.78(含)以前版本
問題描述	CVE-2025-10264(Exposure of Sensitive Information)： 未經身分鑑別之遠端攻擊者可存取系統設定檔並取得該NVR與連線攝影機之明文帳號密碼。

	CVE-2025-10265(OS Command Injection)： 已通過身分鑑別之遠端攻擊者可注入任意作業系統指令並於設備上執行。
解決方法	更新韌體版本至x.x.x.79(含)以後版本
公開日期	2025-09-11
相關連結	**https://www.twcert.org.tw/tw/cp-132-10375-19f1e-1.html**
新人類資訊科技｜NUP Portal - SQL Injection	
TVN / CVE ID	TVN-202509002 / CVE-2025-10266
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	NUP Portal SP5.0(含)以前版本
問題描述	新人類資訊科技開發之NUP Portal存在SQL Injection漏洞，未經身分鑑別之遠端攻擊者可注入任意SQL指令讀取、修改及刪除資料庫內容。
解決方法	更新至SP5.1(含)以後版本
公開日期	2025-09-11
相關連結	**https://www.twcert.org.tw/tw/cp-132-10377-89750-1.html**
金諄資訊｜統計資料庫系統 - Missing Authentication	
TVN / CVE ID	TVN-202509003 / CVE-2025-10452
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	統計資料庫系統1.0.1(不含)以下版本
問題描述	金諄資訊開發之統計資料庫系統存在Missing Authentication漏洞，未經身分鑑別之遠端攻擊者可直接以高權限讀取、修改及刪除資料庫內容。

解決方法	更新至1.0.1(含)以上版本
公開日期	2025-09-15
相關連結	https://www.twcert.org.tw/tw/cp-132-10379-70d40-1.html
新夥伴科技 | N-Reporter, N-Cloud, N-Probe - OS Command Injection	
TVN / CVE ID	TVN-202509005 / CVE-2025-10589
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	受影響產品： N-Reporter, N-Cloud, N-Probe 受影響Firmware版本： 6.x系列之6.1.187(20250730-1734)(不含)以前版本 7.x系列之7.0.009(20250805-1505)(不含)以前版本 受影響Kernel版本： 20250811094737(不含)以前版本
問題描述	新夥伴科技開發之N-Reporter、N-Cloud及N-Probe存在OS Command Injection漏洞，已通過身分鑑別之遠端攻擊者可注入任意作業系統指令並於伺服器上執行。
解決方法	Firmware更新： 6.x版本請更新至6.1.187(20250730-1734)(含)以後版本 7.x版本請更新至7.0.009(20250805-1505)(含)以後版本 Kernel更新： 請更新至 20250811094737(含)以後版本 Firmware 與 Kernel 必須同步更新，以確保修補生效。
公開日期	2025-09-17
相關連結	https://www.twcert.org.tw/tw/cp-132-10386-231ae-1.html
普萊德科技 | 工業級行動通訊閘道器 - 存在2個漏洞	

TVN / CVE ID	TVN-202509006 / CVE-2025-9971, CVE-2025-9972
CVSS	CVE-2025-9971： 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVE-2025-9972： 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	ICG-2510WG-LTE (EU/US) 1.0-20240918(含)以前版本 ICG-2510W-LTE (EU/US) 1.0_20240411(含)以前版本
問題描述	CVE-2025-9971(Missing Authentication)： 未經身分鑑別之遠端攻擊者可利用特定功能對設備進行操作。 CVE-2025-9972(OS Command Injection)： 未經身分鑑別之遠端攻擊者可注入任意作業系統指令並於設備上執行。
解決方法	更新ICG-2510WG-LTE (EU/US)至1.0_20250811(含)以後版本 更新ICG-2510W-LTE (EU/US)至1.0_20250811(含)以後版本
公開日期	2025-09-17
相關連結	**https://www.twcert.org.tw/tw/cp-132-10389-265a3-1.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：**2025年9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/**