TWCERT/CC 資安情資電子報

2025 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

第 1 章、封面故事

FBI和CISA聯合公告LummaC2攻擊手法

2025年5月中旬，美國聯邦調查局(FBI)與美國網路安全暨基礎設施安全局(CISA)聯合發布公告，揭露LummaC2攻擊手法，並公開攻擊者的已知策略、技術和程序(TTP)以及攻擊指標(IoC)。LummaC2是一種資訊竊取惡意軟體，常透過魚叉式釣魚連結和附件，誘使受害者下載並執行惡意payload。攻擊者還會偽造CAPTCHA，誘騙毫無戒心的使用者點擊執行。該CAPTCHA實際上包含指令，會自動開啟windows執行視窗並貼上內容，當受害者按下「Enter」鍵後，惡意的Base64編碼PowerShell腳本即被執行，進而完成攻擊流程。

為了混淆追蹤與規避防禦，攻擊者將LummaC2嵌入偽裝成流行軟體中，藉此繞過端點偵測和回應系統(EDR)及防毒軟體等標準網路安全措施。一旦受害者電腦系統遭感染，LummaC2會自動竊取用戶的敏感資料，包括個人身分訊息、財務憑證、加密貨幣錢包等，對受害者造成嚴重資安威脅。

執行LummaC2.exe後的運作流程可分為以下幾個步驟：

1. 執行LummaC2.exe時，程式會顯示解密對話框，詢問使用者是否繼續操作。選擇「Yes」，程式將進行解密並呼叫命令與控制（C2）網域；若選擇「No」，程式即退出。
2. 解碼後的C2網域會被惡意程式用以發送POST請求。當請求成功時，解碼後的網域字串指標會儲存在全域變數中，供後續檢索與解析JSON格式的回應資料。
3. 程式利用API查詢受害者的使用者帳號名稱和電腦名稱，並將資料進行雜湊處理與比對。若比對成功，則呼叫最終子程式，啟動後續惡意行為。

針對LummaC2等資訊竊取惡意軟體的威脅，企業與個人應持續強化資安防護措施。建議啟用多因子認證(MFA)，有效防止未經授權的帳號登入；同時定期更新作業系統與應用程式，修補已知漏洞以降低攻擊。此外，應加強員工資安教育教育，提升對網路釣魚及社交工程攻擊的辨別與警覺性，並定期進行模擬演練和強化意識。同時，軟體應從官方管道下載，避免使用來路不明或盜版程式，以降低被植入惡意程式的風險。面對不斷演進的資安威脅，唯有多層防禦與持續監控，才能有效降低。

詳細IoC請參考CISA官方公告網址：https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141b

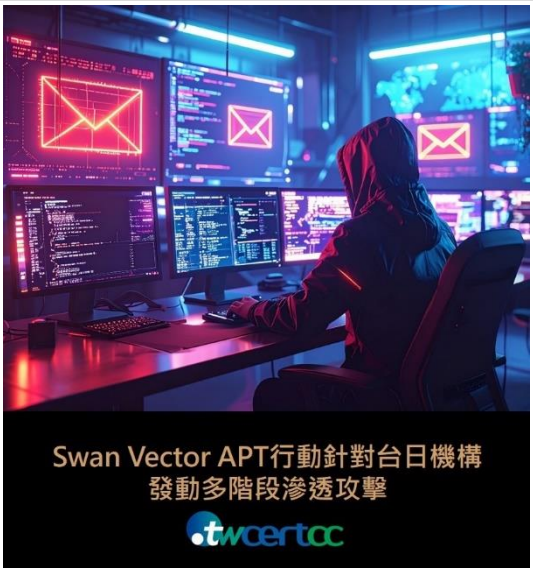
- 相關連結

1. Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations
2. Justice Department Seizes Domains Behind Major Information-Stealing Malware Operation
3. FBI and Europol Disrupt Lumma Stealer Malware Network Linked to 10 Million Infections
4. Lumma infostealer malware operation disrupted, 2,300 domains seized

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 Swan Vector APT行動針對台日機構發動多階段滲透攻擊



Seqrite Labs APT 團隊近期揭露一項名為「Swan Vector」的進階持續性威脅（APT）行動，針對台灣、日本的教育機構與機械工程產業展開網路攻擊。該攻擊活動透過仿真的履歷表與財務文件進行社交工程，誘使受害者點擊釣魚郵件中的附件，進而植入後門程式並取得系統長期控制權。

從初始感染至最終建立遠端控制通道，攻擊採取多階段方式進行。最初的感染載體為壓縮檔「歐買尬金流問題資料_20250413(6).rar」。壓縮檔中包含一個惡意捷徑檔（.lnk）與一個偽裝成圖片的DLL檔案。一旦捷徑被執行，系統便會透過 rundll32.exe執行第一個後門程式Pterois，並從遠端伺服器下載誘餌文件與下一階段載荷。

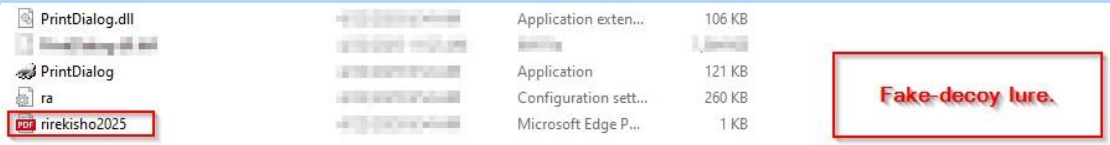


圖1: 下載之PDF誘餌文件。圖片來源：Seqrite

圖2:誘餌文件為日文履歷表。圖片來源：Seqrite

Pterois使用OAuth憑證完成身份驗證，利用Google Drive作為C2通訊平台。其下載的檔案中包含合法的執行檔PrintDialog.exe及惡意DLL（Isurus），兩者結合後便可載入設定檔中的加密shellcode。整個過程透過API混淆與Syscall執行，幾乎不留痕跡，難以偵測。

最終階段則部署Cobalt Strike beacon，與託管於日本的伺服器（IP：52[.]199[.]49[.]4:7284）建立通訊，完成遠端控制通道，進一步實現持續性滲透與資料竊取。

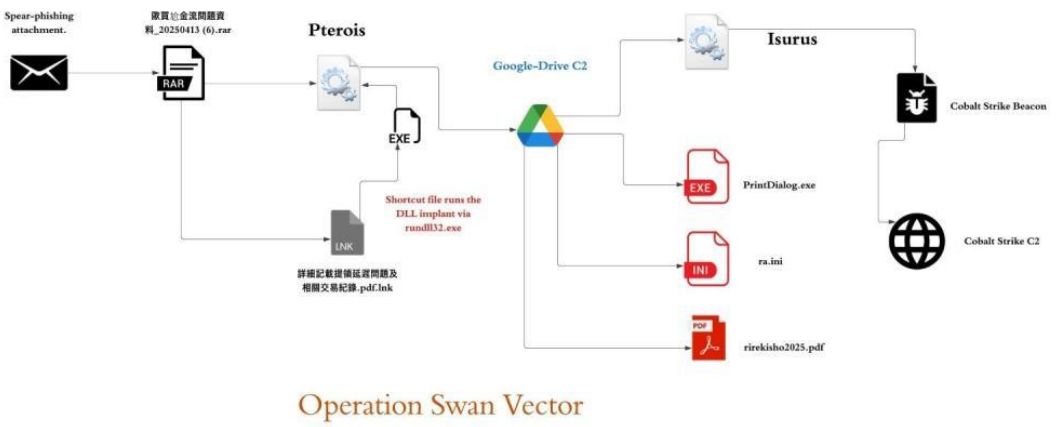


圖3:誘餌文件為日文履歷表。圖片來源：Seqrite

此次行動展現之模組化設計、進階技術（如API混淆、DLL側載、Google Drive濫用、syscall注入）與行動成熟度，整體與Winnti、Lazarus、APT10等東亞知名APT組織存在技術重疊與行為模式相似，結合語言線索與攻擊時間，推測背後攻擊者可能來自東亞地區且長期對特定區域進行持續滲透與情報蒐集。

建議各組織強化釣魚郵件檢測、監控DLL側載行為與異常合法程式使用模式，並加強對LOLBin（Living Off the Land Binaries）濫用、Google Drive非典型OAuth活動之分析與回應。此外，須準備應對策略，以因應未來可能擴及Python、OneDrive Launcher等更多合法應用程序之攻擊變種。

以下為Seqrite提供此次攻擊行為的IoC：

IP: 52[.]199[.]49[.]4

檔案名稱	IoC
PrintDialog.exe	7a942f65e8876aeec0a1372fcd4d53aa1f84d2279904b2b86c49d765e5a29d6f
PrintDialog.dll	a9b33572237b100edf1d4c7b0a2071d68406e5931ab3957a962fcce4bfc2cc49
ra.ini	0f303988e5905dffc3202ad371c3d1a49bd3ea5e22da697031751a80e21a13a7
rirekisho2025.pdf	8710683d2ec2d04449b821a85b6ccd6b5cb874414fd4684702f88972a9d4cfdd
rirekisho2021_01.pdf	8710683d2ec2d04449b821a85b6ccd6b5cb874414fd4684702f88972a9d4cfdd

wbemcomn.dll	c7b9ae61046eed01651a72afe7a31de088056f1c1430b368b1acda0b58299e28
svhost.exe	e0c6f9abfc11911747a7533f3282e7ff0c10fc397129228621bcb3a51f5be980
0g9pglZr74.ini	9fb57a4c6576a98003de6bf441e4306f72c83f783630286758f5b468abaa105d
KpEvjK3KG2.enc	e86feaa258df14e3023c7a74b7733f0b568cc75092248bec77de723dba52dd12
LoggingPlatform.dll	9df9bb3c13e4d20a83b0ac453e6a2908b77fc2bf841761b798b903efb2d0f4f7
python310.dll	e1b2d0396914f84d27ef780dd6fdd8bae653d721eea523f0ade8f45ac9a10faf
ra.ini	777961d51eb92466ca4243fa32143520d49077a3f7c77a2fcbec183ebf975182
pythonw.exe	040d121a3179f49cd3f33f4bc998bc8f78b7f560bfd93f279224d69e76a06e92
python.xml	c8ed52278ec00a6fbc9697661db5ffbcbe19c5ab331b182f7fd0f9f7249b5896
OneDriveFileLauncher.exe	7bf5e1f3e29beccca7f25d7660545161598befff88506d6e3648b7b438181a75
Chen_YiChun.png	de839d6c361c7527eeaa4979b301ac408352b5b7edeb354536bd50225f19cfa5
針對提領系統與客服流程的改進建議.pdf.lnk	9c83faae850406df7dc991f335c049b0b6a64e12af4bf61d5fb7281ba889ca82

詳細IoC請參考Seqrite公告網址：https://www.seqrite.com/blog/swan-vector-apt-targeting-taiwan-japan-dll-implants/

- 相關連結
  1. Unveiling Swan Vector APT Targeting Taiwan and Japan with varied DLL Implants
  2. Swan Vector APT Targets Organizations with Malicious LNK and DLL Implants
  3. Swan Vector APT Hackers Attacking Organizations With Malicious LNK & DLL Implants

2.2 新興應用資安

2.2.1 「你知道公司內部用了多少 AI 工具嗎？」資安新創Harmonic揭露影子AI危機

隨著生成式人工智慧(GenAI)在企業內部的應用迅速擴展，資安團隊面臨前所未有的挑戰。企業除了滿足業務部門加快採用AI工具的需求外，更需嚴格控管隨之而來的資安風險，尤其是敏感資料外洩與合規問題。

目前企業常見的AI風險包括：

- 機密資料被納入其他公司模型訓練中
- 資料流向地緣政治敏感地區
- 員工使用未經授權的AI應用程式

近期案例顯示，一家銀行內部員工使用超過50種未經批准的AI工具，

僅有2種獲得公司授權；另一家科技公司工程師甚至將400GB資料上傳至未授權平台。更有新進員工在完成資安訓練後，將原始碼上傳至中國所屬大型語言模型平台。

企業目前嘗試多種控管措施，但仍面臨挑戰：

- 制定AI使用政策：多數公司已有AI使用政策，但員工閱讀率低，更有趣的是，有些政策本身是用ChatGPT所撰寫，實效有限。
- 成立AI指導委員會：形式上看似完整但缺乏可視性，難以有效監督。
- 資料分類管理：利用Microsoft Purview等工具進行資料標記與分類，但在大規模環境中實施困難。
- 統一AI工具平台：約70%企業推行統一平台（如Microsoft Copilot、Google Gemini），但員工常繞過限制，造成資安與業務部門對立。
- 放任模式 (YOLO Mode)：約30%企業僅封鎖高風險工具，對其採取「眼不見為淨」的策略。

Harmonic Security 執行長 Alastair Paterson 建議企業應從「禁止」走向「安全引導使用」，並提出三大核心建議：

- 瀏覽器端的即時監控：透過瀏覽器擴充套件，即時偵測使用者在AI工具中輸入的提示詞(Prompt)與上傳的附件(如Excel、PDF)，有效掌握風險內容。
- 多樣化的模型管控與策略：針對不同敏感資料類型，導入經微調的開源模型(如LLaMA、Mixtral)，在成本可控下提升偵測準確度。

- 可視化儀表板與行為分析：建立全方位儀表板，協助資安團隊掌握 AI 工具使用狀況，進行風險評估與異常行為分析。

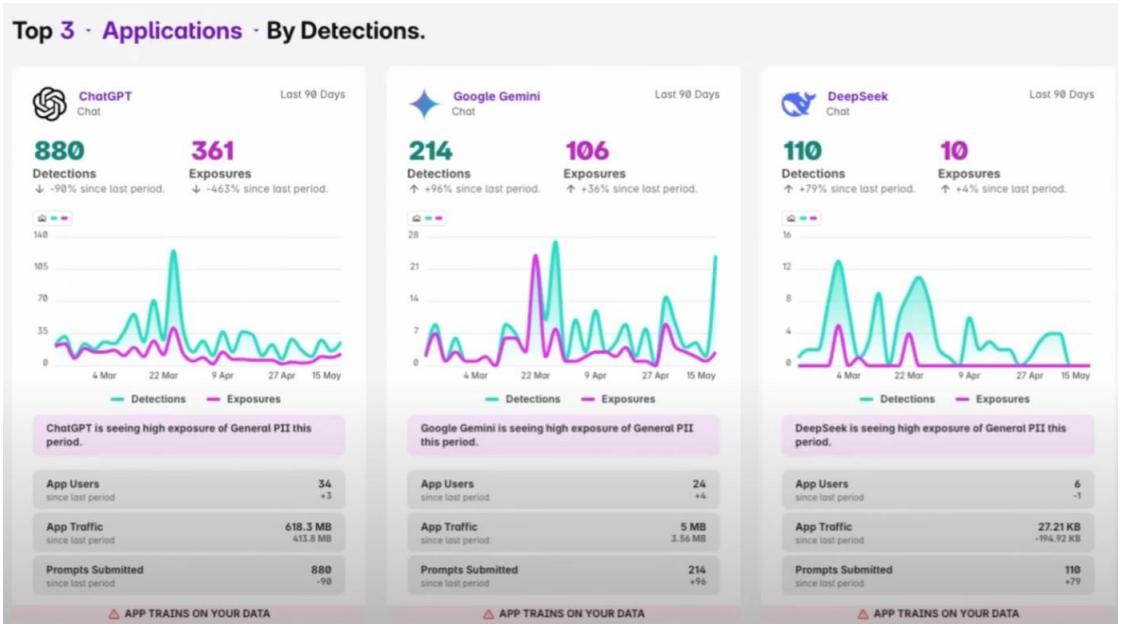


圖1: 視覺化範例。圖片來源：Harmonic Security的展示影片

隨著生成式AI工具持續深入企業日常營運，資安團隊必須從傳統的防堵思維轉型為前瞻性風險治理。唯有結合即時監控、彈性策略與可視化分析，企業才能在追求創新效率的同時，有效控管潛藏的資安威脅，保障企業資訊安全的合規。

- 相關連結
  1. How to Stop Leaking your Sensitive IP to AI Providers with Harmonic Security

2.3 軟硬體漏洞資訊

2.3.1 Cisco 建置於雲端平台的ISE存在憑證漏洞

CVE 編號	CVE-2025-20286
影響產品	Cisco ISE
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-ise-aws-static-cred-FPMjUcm7

- 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。日前 Cisco 發布重大資安漏洞公告(CVE-2025-20286，CVSS：9.9)，此漏洞存在於 AWS、Azure、OCI 雲端部署平台，允許未經身分驗證的遠端攻擊者存取敏感資料、執行有限的管理操作、修改系統配置或破壞受影響系統的服務。

- 影響平台：
  - AWS 平台：ISE 3.1、3.2、3.3、3.4 版本
  - Azure 平台：ISE 3.2、3.3、3.4 版本
  - OCI：ISE 3.2、3.3、3.4 版本
- 資料來源：
  1. Cisco Identity Services Engine on Cloud Platforms Static Credential Vulnerability
  2. CVE-2025-20286

2.3.2 Cisco 整合管理控制器存在權限提升漏洞

CVE 編號	CVE-2025-20261
影響產品	Cisco 整合管理控制器
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-ucs-ssh-priv-esc-2mZDtdjM

- 內容說明：

  Cisco 旗下整合管理控制器(Integrated Management Controller，IMC)是一款專門為 Cisco 整合運算系統的伺服器設計管理工具，提供伺服器遠端監控、配置和管理功能。近日揭露存在一個重大資安漏洞(CVE-2025-20261，CVSS：8.8)，此漏洞存在於 SSH 連線處理中，允許經過身分驗證的遠端攻擊提升存取內部服務權限。

- 影響平台：
  - UCS B-Series Blade Servers
  - UCS C-Series Rack Servers
  - UCS S-Series Storage Servers
  - UCS X-Series Modular System
- 資料來源：
  1. Cisco Integrated Management Controller Privilege Escalation Vulnerability
  2. CVE-2025-20261

2.3.3 Roundcube郵件伺服器存在重大資安漏洞

CVE 編號	CVE-2025-49113
影響產品	Roundcube 郵件伺服器
解決辦法	請更新至 1.6.11、1.5.10(含)之後版本

- 內容說明：

  Roundcube 郵件伺服器是一款開源網頁郵件客戶端，使用者可透過瀏覽器收發電子郵件，廣泛應用於各領域的郵件系統中。近日，Roundcube 開發團隊接獲資安業者通報，指出系統存在重大資安漏洞(CVE-2025-49113，CVSS：9.9)，並已釋出修補更新版本。此漏洞為 PHP 物件反序列化，允許經過身分驗證的攻擊者遠端執行任意程式碼，對系統造成威脅。

- 影響平台：
  - Roundcube 1.1.0 至 1.5.9 版本
  - Roundcube 1.6.0 至 1.6.10 版本
- 資料來源：
  1. Security updates 1.6.11 and 1.5.10 released
  2. Roundcube ≤ 1.6.10 Post-Auth RCE via PHP Object Deserialization [CVE-2025-49113]
  3. CVE-2025-49113

2.3.4 Ivanti 旗下 Ivanti Workspace Control 存在2個重大資安漏洞

CVE 編號	CVE-2025-5353,CVE-2025-22455
影響產品	Ivanti Workspace Control
解決辦法	將 Ivanti Workspace Control (IWC) 更新至 10.19.10.0 版本

- 內容說明：

  Ivanti Workspace Control（IWC）是 Ivanti 旗下的工作區管理解決方案，充當作業系統與用戶之間的中介，用以簡化桌面部署，並保護用戶設定與紀錄。日前，Ivanti 發布資安公告，指出系統存在 2 個重大資安漏洞(CVE-2025-5353，CVSS：8.8 和 CVE-2025-22455，CVSS：8.8)，並釋出修補版本。這 2 個漏洞皆允許經過本地身分驗證的攻擊者，使用硬體編碼金鑰解密儲存的 SQL 憑證。

- 影響平台：
  - Ivanti Workspace Control (IWC) 10.19.0.0 (含)之前版本
- 資料來源：
  1. Security Advisory Ivanti Workspace Control
  2. CVE-2025-5353
  3. CVE-2025-22455

2.3.5 SAP 針對旗下NetWeaver ABAP 應用伺服器修補重大資安漏洞

CVE 編號	CVE-2025-42989
影響產品	SAP NetWeaver ABAP
解決辦法	請至官方網站進行修補：https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2025.html

- 內容說明：

  SAP 針對旗下產品 NetWeaver ABAP 應用程式伺服器發布重大資安漏洞公告(CVE-2025-42989，CVSS：9.6)，此漏洞源於 SAP 遠端功能呼叫(Remote Function Call，RFC)過程中，允許經過身分驗證的攻擊者繞過檢查流程，進而導致提升權限，若成功利用，會嚴重影響應用程式的完整性與可用性。

- 影響平台：
  - KERNEL 7.89、7.93、9.14 、9.15 版本
- 資料來源：
  1. SAP Security Patch Day - June 2025
  2. CVE-2025-42989
  3. CVE-2025-42989

2.3.6 SAP旗下GRC存在重大資安漏洞

CVE 編號	CVE-2025-42982
影響產品	SAP GRC
解決辦法	請至官方網站進行修補：https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2025.html

- 內容說明：

  SAP 針對旗下產品 GRC 發布重大資安漏洞公告(CVE-2025-42982，CVSS：8.8)，此漏洞允許非管理員的使用者存取特定交易，進而可能修改或操控系統傳輸的憑證。若成功利用，會嚴重影響應用程式的機密性、完整性和可用性。

- 影響平台：
  - GRCPINW V1100_700、V1100_731
- 資料來源：
  1. SAP Security Patch Day - June 2025
  2. CVE-2025-42982
  3. CVE-2025-42982

2.3.7 ASUS RT-AX55無線路由器存在安全漏洞，請儘速確認並進行修補

CVE 編號	CVE-2023-39780
影響產品	ASUS RT-AX55 無線路由器
解決辦法	請更新韌體版本至 3.0.0.4.386_51948(含)以後版本

- 內容說明：

  近期研究人員發現有針對 ASUS RT-AX55 無線路由器已知作業系統指令注入(OS command injection)漏洞(CVE-2023-39780)之攻擊行為，對已取得一般權限之遠端攻擊者可於特定參數注入任意作業系統指令並於設備上執行。該漏洞已遭駭客利用，請儘速確認並進行修補。

  備 註 ： CVE-2023-41345 、 CVE-2023-41346 、 CVE-2023-41347 及 CVE-2023-41348 等 4 個漏洞編號等同於 CVE-2023-39780 漏洞，原因為有不同 CVE 核發單位(CNA)對此漏洞核發 CVE 編號，導致此特殊情況。

- 影響平台：
  - RT-AX55 3.0.0.4.386.51598 韌體版本
- 資料來源：
  1. CVE-2023-39780
  2. CVE-2023-41345
  3. CVE-2023-41346
  4. CVE-2023-41347
  5. CVE-2023-41348
  6. ASUS Product Security Advisory

2.3.8 以Chromium為基礎之瀏覽器存在安全漏洞，請儘速確認並進行修補

CVE 編號	CVE-2025-5419
影響產品	以 Chromium 為基礎之瀏覽器
解決辦法	一、請更新 Google Chrome 瀏覽器至 137.0.7151.68(含)以後版本 https://support.google.com/chrome/answer/95414?hl=zh-Hant 二、請更新 Microsoft Edge 瀏覽器至 137.0.3296.62(含)以上版本 https://support.microsoft.com/zh-tw/topic/microsoft-edge-%E6%9B%B4%E6%96%B0%E8%A8%AD%E5%AE%9A-af8aaca2-1b69-4870-94fe-18822dbb7ef1 三、請更新 Vivaldi 瀏覽器至 7.4.3684.50(含)以上版本 https://help.vivaldi.com/desktop/install-update/update-vivaldi/ 四、請更新 Brave 瀏覽器至 1.79.119(含)以上版本 https://community.brave.com/t/how-to-update-brave/384780 五、請更新 Opera 瀏覽器至 119.0.5497.70(含)以上版本 https://help.opera.com/en/latest/crashes-and-issues/#updateBrowser

- 內容說明：

  研究人員發現 Google Chrome、Microsoft Edge、Vivaldi、Brave 及 Opera 等以 Chromium 為基礎之瀏覽器存在堆積溢位(Heap Overflow)漏洞(CVE-2025-5419)，遠端攻擊者可藉由惡意 html 網頁毀損記憶體，進而達到遠端執行任意程式碼或沙箱逃逸。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - Google Chrome 137.0.7151.68(不含)以前版本
  - Microsoft Edge(Based on Chromium) 137.0.3296.62(不含)以前版本
  - Vivaldi 7.4.3684.50(不含)以下版本
  - Brave 1.79.119(不含)以下版本

- Opera 119.0.5497.70(不含)以下版本

- 資料來源：
  1. https://support.google.com/chrome/answer/95414?hl=zh-Hant
  2. https://support.microsoft.com/zh-tw/topic/microsoft-edge-%E6%9B%B4%E6%96%B0%E8%A8%AD%E5%AE%9A-af8aaca2-1b69-4870-94fe-18822dbb7ef1
  3. https://help.vivaldi.com/desktop/install-update/update-vivaldi/
  4. https://community.brave.com/t/how-to-update-brave/384780
  5. https://help.opera.com/en/latest/crashes-and-issues/#updateBrowser
  6. https://nvd.nist.gov/vuln/detail/CVE-2025-5419
  7. https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html
  8. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-5419
  9. https://vivaldi.com/blog/desktop/minor-update-two-7-4/

2.3.9 趨勢科技旗下 Endpoint Encryption PolicyServer 存在多個重大資安漏洞

CVE 編號	CVE-2025-49212,CVE-2025-49213,CVE-2025-49214,CVE-2025-49215,CVE-2025-49216,CVE-2025-49217
影響產品	Trend Micro Endpoint Encryption PolicyServer (TMEE)
解決辦法	更新 Trend Micro Endpoint Encryption (TMEE) PolicyServer 至 6.0.0.4013 (含)版本

- 內容說明：

  Trend Micro Endpoint Encryption PolicyServer (TMEE) 是趨勢科技旗下一款為企業提供 Windows 裝置的全碟與可攜式媒體加密，廣泛應用於需遵循資料保護法規的高管控產業中。近日發布重大資安公告修補多項漏洞：

  【CVE-2025-49212，CVSS：9.8】

  TMEE 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的 TMEE 安裝執行任意程式碼。

  【CVE-2025-49213，CVSS：9.8】

  TMEE 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的 TMEE 安裝執行任意程式碼。

  【CVE-2025-49214，CVSS：8.8】

  攻擊者必須先取得目標系統上執行低權限程式碼權限後，允許經過驗證的攻擊者遠端執行程式碼，執行 TMEE 中的不安全反序列化作業。

  【CVE-2025-49215，CVSS：8.8】

  攻擊者必須先取得目標系統上執行低權限程式碼權限後，允許經過驗證的攻擊者使用 SQL 注入漏洞影響安裝的權限。

【CVE-2025-49216，CVSS：9.8】

此漏洞允許繞過身分驗證的攻擊者，以管理員身分存取關鍵方法並修改產品配置。

【CVE-2025-49217，CVSS：9.8】

TMEE 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的 TMEE 安裝執行任意程式碼。

- 影響平台：
  - Trend Micro Endpoint Encryption (TMEE) PolicyServer 6.0.0.4013 (不含)之前版本
- 資料來源：
  1. CRITICAL SECURITY BULLETIN: Trend Micro Endpoint Encryption PolicyServer (June 2025)
  2. CVE-2025-49212
  3. CVE-2025-49213
  4. CVE-2025-49216
  5. CVE-2025-49217

2.3.10 趨勢科技旗下 Trend Micro Apex Central 存在2個重大資安漏洞

CVE 編號	CVE-2025-49219,CVE-2025-49220
影響產品	Trend Micro Apex Central
解決辦法	請至官方網站進行修補：https://success.trendmicro.com/en-US/solution/KA-0019926

- 內容說明：

  Trend Micro Apex Central 是趨勢科技旗下一款集中式管理平台，用於管理多種 Trend Micro 安全解決方案，包括閘道、郵件伺服器、檔案伺服器和企業桌面。日前發布重大資安公告修補 2 項漏洞：

  【CVE-2025-49219，CVSS：9.8】

  Trend Micro Apex Central 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的 Apex Central 安裝執行任意程式碼。

  【CVE-2025-49220，CVSS：9.8】

  Trend Micro Apex Central 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的 Apex Central 安裝執行任意程式碼。

- 影響平台：
  - Apex Central 2019 (On-prem)(含)之前版本
  - Apex Central as a Service SaaS
- 資料來源：
  1. CRITICAL SECURITY BULLETIN: Trend Micro Apex Central (June 2025)
  2. CVE-2025-49219
  3. CVE-2025-49220

2.3.11 Veeam旗下Veeam Backup & Replication備份軟體存在重大資安漏洞

CVE 編號	CVE-2025-23121
影響產品	Veeam Backup & Replication
解決辦法	請更新至 Veeam Backup & Replication 12.3.2

- 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-2025-23121，CVSS：9.9)允許經網域驗證的使用者，在備份伺服器上可遠端執行任意程式碼。

- 影響平台：
  - Veeam Backup & Replication 12.3.1.1139 (含)之前版本
- 資料來源：
  1. Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2
  2. CVE-2025-23121

2.3.12 Tenable 的 Nessus Agent 存在重大資安漏洞

CVE 編號	CVE-2025-36633
影響產品	Tenable Nessus Agent
解決辦法	請更新至 Tenable Agent 10.8.5 版本

- 內容說明：

  Tenable 提供廣泛部署的弱點掃描工具 Nessus，並提供全球首個可在任何平台上查看維護數位資產安全的曝險管理平台。近日 Tenable 發布重大資安公告(CVE-2025-36633，CVSS：8.8)，此漏洞在 Windows 主機上，Nessus Agent 10.8.5(不含)之前版本中，非管理員使用者可使用 SYSTEM 權限任意刪除本機系統文件，導致本機權限提升。

- 影響平台：
  - Tenable Agent 10.8.5 (不含)之前版本
- 資料來源：
  1. [R1] Nessus Agent Version 10.8.5 Fixes Multiple Vulnerabilities
  2. CVE-2025-36633
  3. CVE-2025-36633

2.3.13 Citrix旗下NetScaler ADC 和 NetScaler Gateway 存在重大資安漏洞

CVE 編號	CVE-2025-5777
影響產品	NetScaler ADC 、 NetScaler Gateway
解決辦法	請更新至以下版本： NetScaler ADC 和 NetScaler Gateway 14.1-43.56 (含)之後版本 NetScaler ADC 和 NetScaler Gateway 13.1-58.32 (含)之後版本 NetScaler ADC 13.1-FIPS 與 NDcPP 13.1-37.235-FIPS 與 NDcPP (含)之後版本 NetScaler ADC 12.1-FIPS 12.1-55.328-FIPS (含)之後版本

- 內容說明：

  Citrix 旗下 NetScaler ADC (原名為 Citrix ADC)是一款網路設備，專為優化、保護及管理企業應用程式與雲端服務而設計；NetScaler Gateway (原名為 Citrix Gateway)則提供安全的遠端存取解決方案，讓使用者能夠從任何地點安全存取應用程式和資料。近日，Citrix 發布重大資安漏洞公告(CVE-2025-5777，CVSS 4.x：9.3)，此為越界讀取漏洞，起因為輸入驗證不足導致記憶體溢位。

  備註：受影響產品 NetScaler ADC 和 NetScaler Gateway 12.1 和 13.0 已是 EoL(End of Life)的產品，Citrix 建議升級至支援版本

- 影響平台：
  - NetScaler ADC 和 NetScaler Gateway 14.1-43.56 (不含)之前版本
  - NetScaler ADC 和 NetScaler Gateway 13.1-58.32 (不含)之前版本
  - NetScaler ADC 13.1-FIPS 與 NDcPP 13.1-37.235-FIPS 與 NDcPP (不含)之前版本
  - NetScaler ADC 12.1-FIPS 12.1-55.328-FIPS (不含)之前版本

- 資料來源：
  1. NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-5349 and CVE-2025-5777
  2. CVE-2025-5777

2.3.14 Cisco 旗下身分識別服務存在二個重大資安漏洞

CVE 編號	CVE-2025-20281,CVE-2025-20282
影響產品	Cisco ISE 、 ISE-PIC
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-ise-unauth-rce-ZAd2GnJ6

- 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。前日 Cisco 發布重大資安漏洞公告(CVE-2025-20281，CVSS：9.8 和 CVE-2025-20282，CVSS：10.0)並釋出更新版本。

  【CVE-2025-20281，CVSS：9.8】

  此漏洞存在於 Cisco ISE 和 Cisco ISE-PIC 的特定 API，攻擊者無需任何有效憑證即可利用此漏洞。允許未經身分驗證的遠端攻擊者以 root 身分在底層作業系統上執行任意程式碼。

  【CVE-2025-20282，CVSS：10.0】

  此漏洞存在於 Cisco ISE 和 Cisco ISE-PIC 的內部 API，允許未經身分驗證的遠端攻擊者將任意檔案上傳至受影響的設備，以 root 身分在底層作業系統執行檔案。

- 影響平台：
  - 【CVE-2025-20281】Cisco ISE 和 ISE-PIC 3.3、3.4 版本
  - 【CVE-2025-20282】Cisco ISE 和 ISE-PIC 3.4 版本
- 資料來源：
  1. Cisco Identity Services Engine Unauthenticated Remote Code Execution Vulnerabilities

2. CVE-2025-20281
3. CVE-2025-20282

2.3.15 Citrix旗下NetScaler ADC 和 NetScaler Gateway 存在重大資安漏洞

CVE 編號	CVE-2025-6543
影響產品	NetScaler ADC 、 NetScaler Gateway
解決辦法	NetScaler ADC 和 NetScaler Gateway 14.1-47.46 (含)之後版本 NetScaler ADC 和 NetScaler Gateway 13.1-59.19 (含)之後版本 NetScaler ADC 13.1-FIPS 與 NDcPP 13.1-37.236-FIPS 與 NDcPP (含)之後版本

- 內容說明：

  Citrix 旗下 NetScaler ADC (原名為 Citrix ADC)是一款網路設備，專為優化、保護及管理企業應用程式與雲端服務而設計；NetScaler Gateway (原名為 Citrix Gateway)則提供安全的遠端存取解決方案，讓使用者能夠從任何地點安全存取應用程式和資料。近日，Citrix 發布重大資安漏洞公告(CVE-2025-6543，CVSS 4.x：9.2)，此為記憶體溢位漏洞，可能導致非預期的控制流程改變和服務阻斷。

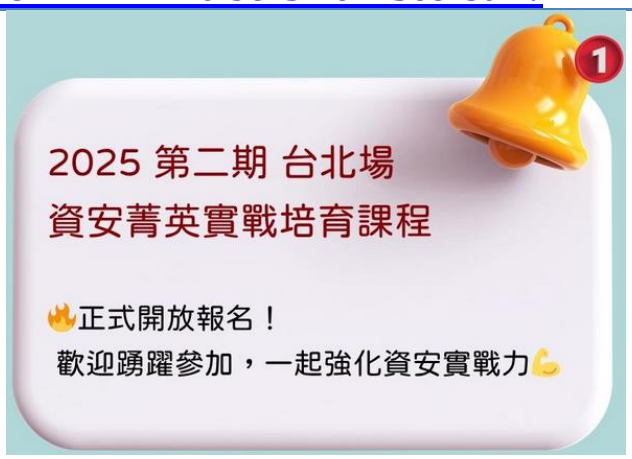
  備註：受影響產品 NetScaler ADC 和 NetScaler Gateway 12.1 和 13.0 已是 EoL(End of Life)的產品，Citrix 建議升級至支援版本

- 影響平台：
  - NetScaler ADC 和 NetScaler Gateway 14.1-47.46 (不含)之前版本
  - NetScaler ADC 和 NetScaler Gateway 13.1-59.19 (不含)之前版本
  - NetScaler ADC 13.1-FIPS 與 NDcPP 13.1-37.236-FIPS 與 NDcPP (不含)之前版本
- 資料來源：
  1. NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-6543
  2. CVE-2025-6543

第 3 章、資安研討會及活動

- **資安研討會**

【資安學院】7/3-7/4、7/7-7/9 ISO/IEC 27001:2022 資訊安全管理系統 CQI & IRCA 主導稽核員訓練課程(課程編號：2535)	
活動時間	2025-07-03 09:00 ~ 2025-07-09 18:30
活動地點	中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）
活動網站	https://www.cisanet.org.tw/Course/Detail/5429
活動概要	 【費用】 原價：56,000元/人 早鳥價：53,000元/人(開課前兩個月) 軟協會員：請電洽承辦人 費用含稅、教材、餐點及完課證明 報名截止： 2025-06-26 【活動內容 / Event Deails】 ISO/IEC 27001 是各國企業組織展現資訊安全管理能力的最佳證明，行政院資通安全會報也以此作為對政府單位之資訊安全要求的準

	則。取得此張證照，不僅肯定個人在資安管理上建置與稽核專業，更展現組織具有資安專業種子人才的能力！ **【主辦單位】中華民國資訊軟體協會** **【聯絡窗口】02-2553-3988 分機 816 林專員** **security@cisanet.org.tw**
【資安院】7/5、7/6、7/12、7/13 資安菁英實戰培育課程-第二期(臺北場)	
活動時間	**2025/7/5、7/6、7/12、7/13**
活動地點	**IEAT會議中心（台北市中山區松江路350號）**
活動網站	**https://www.nics.nat.gov.tw/latest_news/announcements/Event_Information/09cbaeff-7774-4f20-9e43-1d2756e29af2/**
活動概要	 **【費用】** 免費 報名截止： 2025-06- 10 **【報名方式】** 報名表單： https://docs.google.com/forms/d/e/1FAIpQLSd5u4zaylNwAm6prfsZhGhjklyj1qTxOX9U6Z1EqE-OWqmckw/viewform **【參加對象及資格】** 1. 具中華民國國籍，並擁有資安領域 2 年以上實務工作經驗。 2. 以現職政府單位資安技術人員、企業資安技術人員、資安公司研發人員為主要對象，但不限於此範圍。

	3. 完成報名後，資安院將進行資格審查，獲得錄取通知後即可參與全額補助課程。 **【課程內容 / Event Deails】** 資安技術日新月異，真正能守護國家與組織核心資產的，是具備實戰應變能力的資安人才！資安院推出《Cyber Incident Responder 資安事件工程師》實戰菁英培訓課程，由具備國際實務經驗的講師親授，帶領學員深入攻防現場，實作應變流程，培養關鍵戰力 本梯次為今年度最後一場，課程聚焦於惡意程式分析、APT 事件調查與網路威脅防禦競賽，並透過演練平台，全面強化實戰應變技能。課程全程採實體授課，名額有限，誠摯邀請有志投入資安防禦工作的您，一同精進技術、強化應變戰力！ **【課程主題與日期】** ● 07 月 05 日(六) ：以開源工具調查潛伏威脅實務 ● 07 月 06 日(日)：解構野外惡意程式隨開即用的瑞士刀 ● 07 月 12 日(六)：APT 資安事件調查 ● 07 月 13 日(日)：網路威脅防禦競賽 **【主辦單位】**國家資通安全研究院 **【聯絡窗口】02-6631-3526 陳小姐**
【數位產業署】7/9 AI應用下的資安風險	
活動時間	**2025/07/09(三) 13:30-17:00**
活動地點	**Teams線上**
活動網站	**https://ievents.iii.org.tw/eventS.aspx?t=0&id=2851**

活動概要	 **【費用】** 免費 報名截止：2025/07/04 **【課程目標 / Event Deails】** 1. 了解 AI Chatbot 如何影響我們的日常生活與工作。 2. 認識使用 AI 時可能遇到的幾種主要資安風險（例如：被誘導說出不該說的話、 看到假訊息等）。 3. 透過實際生活案例，了解 AI 風險的具體樣貌。 4. 學習保護個人資訊、辨識 AI 風險的基本方法。 5. 提升在日常使用 AI 工具時的警覺心與安全意識。 **【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】0920795301 陳小姐** **yuxuanchen@iii.org.tw**
【資安學院】7/12、7/19 iPAS-「中級」資訊安全工程師-能力研習衝刺班	
活動時間	**7/12、7/19 09:00 ~ 16:00**
活動地點	**中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/5437**

活動概要	 **【費用】** 原價：12,000元/人 軟協會員：9,000元/人 早鳥價：11,000元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025/07/05 **【活動內容 / Event Deails】** 本課程融入業界實務案例，教授專業的資訊安全知識與技能，如建立符合法規與組織安全需求之系統、網路與安全防護架構、執行相關維運作業等，課程中亦透過歷屆試題講解重點觀念，協助您掌握 iPAS 考題趨勢及技術解析，不僅提升解題戰力，應考也更佳輕鬆！ **【主辦單位】中華民國資訊軟體協會** **【聯絡窗口】02-2553-3988 分機 816 林專員** **security@cisanet.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：

宏頂科技 智慧停車管理系統 - Exposure of Sensitive Information	
TVN / CVE ID	TVN-202506002 / CVE-2025-5893
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	智慧停車管理系統1.0至1.4版本
問題描述	宏頂科技智慧停車管理系統存在Exposure of Sensitive Information漏洞，未經身分鑑別之遠端攻擊者可存取特定頁面取得管理權限明文帳號密碼。
解決方法	更新至1.5(含)以後版本
公開日期	2025-06-09
相關連結	**https://www.twcert.org.tw/tw/cp-132-10167-39c6d-1.html**
宏頂科技 智慧停車管理系統 - Missing Authorization	
TVN / CVE ID	TVN-202506003 / CVE-2025-5894
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	智慧停車管理系統 1.0 至 1.4 版本
問題描述	宏頂科技智慧停車管理系統存在Missing Authorization漏洞，已取得一般權限之遠端攻擊者可存取特定功能新增管理者帳號，並使用該帳號登入系統。
解決方法	更新至1.5(含)以後版本
公開日期	2025-06-09
相關連結	**https://www.twcert.org.tw/tw/cp-132-10170-e2435-1.html**

Acer ControlCenter - Remote Code Execution	
TVN / CVE ID	TVN-202506004 / CVE-2025-5491
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	ControlCenter 4.00.3000 至 4.00.3056版本
問題描述	Acer ControlCenter 存在Remote Code Execution漏洞。該程式透過自訂的 Windows Named Pipe 對外提供功能。然而該 Named Pipe 配置不當，使得具備低權限之遠端使用者也能與其互動並存取相關功能。其中一項功能允許以 NT AUTHORITY/SYSTEM 身分執行任意程式，攻擊者可藉此在目標系統上以高權限執行任意程式碼。
解決方法	更新至4.00.3058(含)以後版本
公開日期	2025-06-13
相關連結	**https://www.twcert.org.tw/tw/cp-132-10180-36818-1.html**

哈瑪星科技 WIMP 網站共構管理平台 - SQL Injection	
TVN / CVE ID	TVN-202506005 / CVE-2025-6169
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	WIMP 網站共構管理平台 5.3.1.34642(含)以前版本
問題描述	哈瑪星科技WIMP網站共構管理平台存在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 5.3.1.34643(含)以後版本
公開日期	2025-06-16
相關連結	**https://www.twcert.org.tw/tw/cp-132-10183-99ce1-1.html**

金智洋科技 無線分享器 - OS Command Injection	
TVN / CVE ID	TVN-202506006 / CVE-2025-6559
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	影響型號： BR071n, BR261c, BR270n, BR476n, BRC70n, BRC70x, BRC76n, BRD70n, BRE70n, BRE71n, BRF61c, BRF71n
問題描述	金智洋科技多個無線分享器型號存在OS Command Injection漏洞，允許未經身分鑑別之遠端攻擊者注入任意作業系統指令並於設備上執行。
解決方法	受影響型號已不再維護，建議汰換設備
公開日期	2025-06-24
相關連結	https://www.twcert.org.tw/tw/cp-132-10196-898d3-1.html
金智洋科技 無線分享器 - Exposure of Sensitive Information	
TVN / CVE ID	TVN-202506007 / CVE-2025-6560
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	影響型號： BR071n, BR261c, BR270n, BR476n, BRC70n, BRC70x, BRC76n, BRD70n, BRE70n, BRE71n, BRF61c, BRF71n
問題描述	金智洋科技部分無線分享器型號存在Exposure of Sensitive Information漏洞，未經身分鑑別之遠端攻擊者可直接存取系統設定檔案取得管理者明文帳號密碼。
解決方法	受影響型號已不再維護，建議汰換設備
公開日期	2025-06-24
相關連結	https://www.twcert.org.tw/tw/cp-132-10197-524ea-1.html
杭特電子 混合式監視系統主機 - Exposure of Sensitive System Information	

TVN / CVE ID	TVN-202506008 / CVE-2025-6561
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	影響型號：HBF-09KD、HBF-16NK 影響韌體版本：V3.1.67_1786 BB11115(含)以前版本
問題描述	杭特電子部分混合式監視系統主機型號(HBF-09KD與HBF-16NK)存在Exposure of Sensitive Information漏洞，未經身分鑑別之遠端攻擊者可直接存取系統設定檔案取得管理者明文帳號密碼。
解決方法	更新韌體版本至V3.1.70_1806 BB50604(含)以後版本
公開日期	2025-06-24
相關連結	**https://www.twcert.org.tw/tw/cp-132-10199-9c5c6-1.html**
杭特電子 混合式監視系統主機 - OS Command Injection	
TVN / CVE ID	TVN-202506009 / CVE-2025-6562
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	響型號：HBF-09KD、HBF-16NK 影響韌體版本：V3.1.67_1786 BB11115(含)以前版本
問題描述	杭特電子部分混合式監視系統主機型號(HBF-09KD與HBF-16NK)存在OS Command Injection漏洞，允許已取得一般權限之遠端攻擊者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V3.1.70_1806 BB50604(含)以後版本
公開日期	2025-06-24
相關連結	**https://www.twcert.org.tw/tw/cp-132-10201-044e9-1.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/**