TWCERT/CC 資安情資電子報

2026 年 1 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

「Contagious Interview」攻擊手法再進化：濫用 VS Code Tasks 建立持久化機制

資安研究團隊OSM(OpenSourceMalware)與Palo Alto Networks近期發布聯合警訊，指出駭客組織發起的「Contagious Interview(傳染性面試)」行動出現重大技術演變。攻擊者不再僅依賴誘騙受害者手動執行惡意檔案，而是轉向濫用開發工具Visual Studio Code (VS Code)內建的tasks.json自動化機制。只要開發者在受信任模式下開啟惡意專案資料夾，無須手動編譯或執行程式，惡意指令即會在背景自動觸發，大幅提高了攻擊的隱蔽性。

這波攻擊主要鎖定加密貨幣產業的軟體工程師與自由接案者。攻擊者首先在LinkedIn、Upwork 或 Fiverr等求職與外包平台偽裝成招募人員或雇主 。他們以高薪職缺或新專案為誘因，主動接觸警覺性較低的開發者。

在取得信任後，攻擊者會要求工程師從GitHub或GitLab下載一個專案進行測試，當工程師使用VS Code開啟該專案資料夾時，主要核心的滲透技術如下：

- 埋藏惡意配置：攻擊者在專案的 .vscode資料夾中植入惡意tasks.json檔案
- 濫用自動化屬性：該設定檔使用了 runOn: folderOpen 屬性。這意味著只要 VS Code 開啟該資料夾，定義好的惡意任務就會自動執行
- 利用「信任」心理：當VS Code彈出「Workspace Trust(工作區信任)」提示詢問是否信任作者時，若急於求職的受害者點選「是(Yes)」，系統將直接放行自動化任務
- 跨平台感染：任務觸發後，系統會根據受害者的作業系統(Windows 、 macOS 或 Linux)自動下載對應的引導程式(Bootstrapper)，建立持久化機制並載入後續惡意模組

這類攻擊利用開發者對Visual Studio Code等工具的信任，誘使受害者下載看似正常的專案並點選「信任作者」。與 ClickFix 需要引導使用者手動貼上代碼不同，IDE 攻擊透過軟體內建的自動化任務執行惡意指令，其高度隱蔽性與「合法化」操作，被專家視為下一波針對性攻擊(APT)的初始感染主流

透過上述機制植入的惡意程式，已被識別為 **BeaverTail 最新變種**

（**Type 701**），並呈現與 **OtterCookie** 的功能融合趨勢（部分分析將其稱為 **OtterCandy**）。一旦惡意任務啟動，系統會依據受害者作業系統（Windows、macOS 或 Linux）下載對應的引導程式（bootstrapper），最終在電腦上落地執行高度混淆的 JavaScript 惡意程式 BeaverTail（Type 701）。

該版本的 BeaverTail 能力大幅提升，主要以竊取資訊為目的，至少可針對 43 種以上與加密貨幣相關的瀏覽器擴充功能（例如 MetaMask、Phantom 等）與多家錢包服務供應商進行資料竊取；同時也會竊取登入憑證、Session Cookie、LocalStorage 以及瀏覽器內的 LevelDB（.ldb）等高度敏感資料。

面對針對開發環境的供應鏈攻擊，資安專家建議企業與開發者採取以下防護措施：

1. 開啟不明來源的程式碼庫時，避免輕易點選VS Code的「信任」選項
2. 定期檢查 .vscode/tasks.json 是否存在異常或自動執行的設定
3. 建議將開發環境與日常使用帳號進行權限分離，以降低風險
4. 部署郵件閘道掃描機制與 VS Code 擴展功能白名單，並限制或停用不必要的任務自動執行功能
5. 加密產業相關人員應特別提高警覺，並搭配端點防護與行為監控機制

- 相關連結
  1. Latest Contagious Interview malware campaign abuses Microsoft VSCode Tasks
  2. BeaverTail and OtterCookie evolve with a new Javascript module
  3. Hacking Employers and Seeking Employment
  4. North Korean Hackers Combine BeaverTail and OtterCookie into Advanced JS Malware

第 2 章、國內外重要資安事件

2.1 軟硬體系統資安議題

2.1.1 MongoDB伺服器面臨MongoBleed記憶體資料外洩風險

近期MongoDB公布一項高風險資安漏洞CVE-2025-14847(CVSS 4.x：8.7)，影響多個MongoDB伺服器版本，近期已被證實遭攻擊者積極利用，全球逾8.7萬台對外公開的伺服器可能面臨敏感資料外洩風險。該漏洞源於驗證參數長度時處理不當，允許未經身分驗證的遠端攻擊者可傳送精心設計的zlib壓縮通訊封包，藉此取得記憶體中的敏感資料，包括資料庫密碼、存取金鑰、憑證及其他敏感資料。

美國網路安全暨基礎設施安全局(CISA)已於2025年12月29日將此漏

洞納入已知利用漏洞(KEV）目錄，提醒企業與政府機關優先修補。由於PoC程式碼已公開，資安研究人員建議立即套用官方修補程式；若短期內無法立即套用修補程式，建議採取的應變措施包括：暫時停用MongoDB的zlib壓縮功能、重新評估伺服器對外開放的必要性，並同步加強日誌監控，以即時發現異常的認證或連線行為。

技術細節顯示，CVE-2025-14847發生於MongoDB Server處理zlib壓縮訊息並進行解壓時，對「解壓後資料長度」的回報/處理出現錯誤：系統誤以已配置的緩衝區大小為有效資料長度，而非實際解壓後的資料長度，導致回應中可能夾帶未初始化的堆（heap）記憶體殘留資料。攻擊者可透過送出特製請求反覆觸發此行為，逐次取得不同的記憶體片段，累積後有機會拼湊出敏感資訊(如憑證、金鑰或Token等)。該漏洞具備「洩漏記憶體殘留資料」的特性，被研究人員命名為「MongoBleed」，如圖1實驗結果所示。

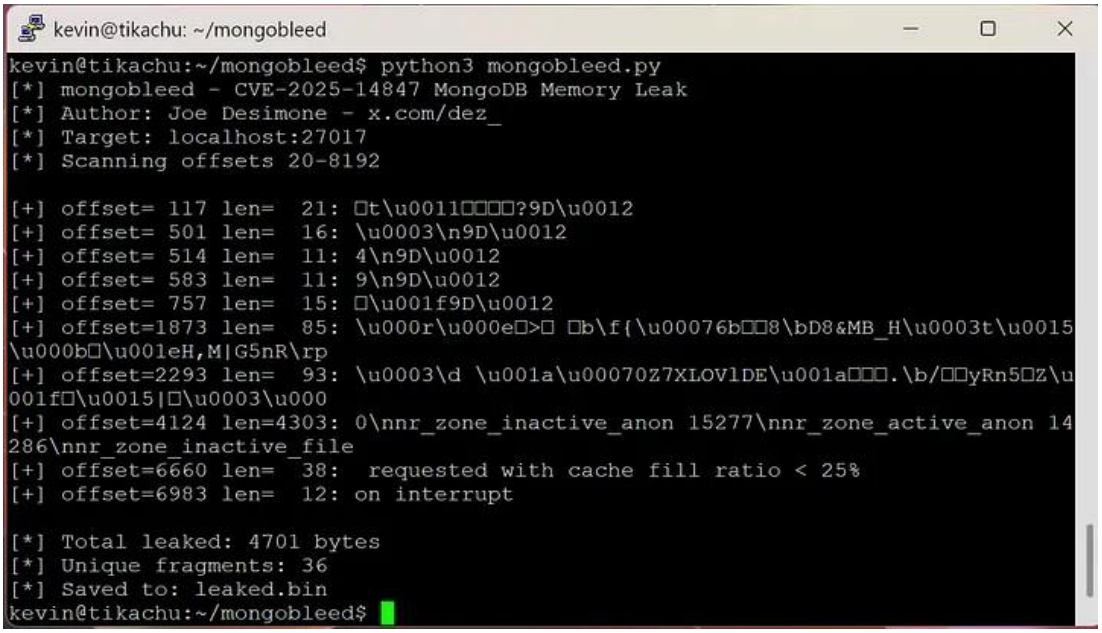


圖1：MongoBleed漏洞導致敏感資料外洩的實驗結果。圖片來源：Kevin Beaumont

以下是根據這次漏洞的建議和防護措施：

1. 盤點現有MongoDB版本與系統設定，確認是否屬於受影響範圍
2. 優先更新至官方已修補版本(8.2.3、8.0.17、7.0.28、6.0.27、5.0.32 或 4.4.30)；已停止支援的舊版系統，應儘速升級或汰換為可獲得安全更新版本。若無法立即修補，應暫時停用zlib壓縮或改用其他壓縮機制
3. 部署入侵防禦系統(IPS)及Web應用防火牆(WAF)，以攔截異常或畸形zlib封包請求，並持續監控可疑流量
4. 加強內部監控與異常行為分析機制，限制MongoDB直接暴露於網路
5. 啟用身份驗證及網路隔離措施，以降低遭入侵與資料外洩的風險

- 相關連結
  1. MongoBleed (CVE-2025-14847): MongoDB Memory Leak Flaw
  2. MongoDB Unauthenticated Attacker Sensitive Memory Leak
  3. Exploited MongoBleed flaw leaks MongoDB secrets, 87K servers exposed
  4. MongoDB Vulnerability CVE-2025-14847 Under Active Exploitation Worldwide
  5. Merry Christmas Day! Have a MongoDB security incident.
  6. December 27 Advisory: MongoBleed - Critical MongoDB Uninitialized Memory Disclosure Vulnerability [CVE-2025-14847]
  7. Make minimally sized buffers for uncompressed Messages

2.1.2 n8n自動化平台存在多項嚴重漏洞，呼籲用戶立即更新版本

近期，開源工作流程自動化工具n8n平台，揭露四項嚴重資安漏洞。這些漏洞可能導致未經授權的遠端程式碼執行(RCE)或敏感資料外洩，影響多n8n版本。由於n8n在許多企業中扮演著自動化基礎架構的「中樞神經」，集中管理 API 金鑰、OAuth Token 及資料庫帳密等高度敏感的憑證，一旦遭受入侵，攻擊者恐藉此橫向滲透企業內部網路，甚至發動大規模的供應鏈攻擊，n8n 團隊已緊急釋出修補版本，並強烈呼籲所有用戶儘速完成更新。

以下是近期揭露的漏洞詳情概述：

CVE-2026-21858 (CVSS: 10.0) – 「Ni8mare」，影響版本為(>= 1.65.0 <1.121.0)：此漏洞允許未經身分驗證的攻擊者，透過 Webhook 處

理過程中的「Content-Type 混淆」缺陷，繞過檔案上傳解析器並覆蓋「req.body.files」變數。攻擊者可藉此讀取伺服器上的任意檔案(例如資料庫與設定檔)，竊取加密金鑰後偽造管理員 Session Cookie，進而利用該權限建立惡意工作流程，執行任意程式碼 (RCE)，最終接管n8n行程權限。

CVE-2025-68668 (CVSS: 9.9) – 「N8scape」，影響版本為(>= 1.0.0 <2.0.0)：這是一個 Python沙箱逃逸漏洞。經過身分驗證的攻擊者，可利用 Python 節點中 Pyodide 環境與 JavaScript 之間的互操作機制，繞過既有的沙箱限制。攻擊者進而呼叫未授權限制的 Node.js 內部 API(如 child_process)，並以n8n服務行程的權限執行任意作業系統指令，最終可能導致遠端程式碼執行風險。

CVE-2026-21877 (CVSS: 10.0) ，影響版本為(>= 0.121.2)：此漏洞存在於 Git 節點功能中。由於對儲存庫路徑缺乏足夠的驗證，經過身分驗證的攻擊者可藉由惡意路徑操控檔案系統，並執行惡意程式碼。影響範圍涵蓋自託管及雲端版本的 n8n 平台。

CVE-2025-68613 (CVSS: 9.9) ，影響版本為(>= 0.211.0 <1.120.4)：此漏洞允許經過身分驗證的攻擊者，透過表達式注入惡意遠端程式碼。由於缺乏適當的隔離，攻擊者可透過「全域 this」上下文存取 process.mainModule.require，進而載入系統模組執行指令。

為有效應對此高風險威脅，企業和組織應立即採取以下防護措施：

1. **立即更新版本**：務必依循n8n官方安全公告，確認自身使用版本是否受影響，並儘速升級至已修補漏洞的安全版本。
2. **限制網路存取範圍**：除非有明確業務需求，應避免將n8n相關服務直接暴露於網際網路。建議僅允許透過VPN或內部網路存取，

並強制啟用身分驗證機制或多因子驗證（MFA）。

3. **暫時停用高風險功能**：若無法立即更新，可透過環境變數(例如NODES_EXCLUDE)暫時停用Code Node 或Git Node，或設定「N8N_PYTHON_ENABLED=false」以關閉 Python 執行功能，藉此降低可被利用的攻擊面。
4. **強化日誌監控與鑑識**：持續監控n8n的工作流程日誌與系統行為，特別留意是否有異常的「child_process」建立、不明的檔案系統寫入，或工作流程中包含可疑的 JavaScript 表達式。

- 相關連結
  1. Critical n8n Vulnerability (CVSS 10.0) Allows Unauthenticated Attackers to Take Full Control
  2. n8n CVE-2025-68613 RCE Exploitation: A Detailed Guide
  3. CVE-2025-68668: Breaking Out of the Python Sandbox in n8n
  4. CVE-2026-21877: n8n Workflow Automation RCE Vulnerability
  5. Ni8mare - Unauthenticated Remote Code Execution in n8n (CVE-2026-21858)
  6. Security - n8n

2.2 軟硬體漏洞資訊

2.2.1 PostgreSQL圖形化介面工具pgAdmin存在高風險安全漏洞(CVE-2025-13780)

CVE 編號	CVE-2025-13780
影響產品	PostgreSQL pgAdmin
解決辦法	更新 pgAdmin 至 9.11(含)以上版本

- 內容說明：

  研究人員發現 PostgreSQL 圖形化介面工具 pgAdmin 存在程式碼注入(Code Injection)漏洞(CVE-2025-13780)。當系統處於伺服器模式(Server Mode)下，取得一般權限之遠端攻擊者可上傳特製惡意備份檔，後續當觸發 PLAIN 格式備份檔還原功能時，系統會解析特製備份檔，進而於 pgAdmin 主機上執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - pgAdmin 9.10(含)以下版本
- 資料來源：
  1. CVE-2025-13780
  2. When Regex Isn't Enough: How We Discovered CVE-2025-13780 in pgAdmin

2.2.2 Digiever DS-2105 Pro存在高風險安全漏洞(CVE-2023-52163)

CVE 編號	CVE-2023-52163
影響產品	Digiever DS-2105 Pro
解決辦法	官方針對已停止支援(EOL)之設備提出安全建議，請參考官方說明，網址如下： https://www.digiever.com/tw/support/faq-content.php?FAQ=217

- 內容說明：

  研究人員發現 Digiever DS-2105 Pro 存在作業系統指令注入(OS Command Injection)漏洞(CVE-2023-52163)。取得一般權限之遠端攻擊者可將惡意指令注入 time_tzsetup.cgi，進而執行遠端程式碼。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - Digiever DS-2105 Pro 3.1.0.71-11
- 資料來源：
  1. CVE-2023-52163
  2. DIGIEVER 資安更新通知

2.2.3 Veeam旗下Veeam Backup & Replication備份軟體存在重大資安漏洞(CVE-2025-59470)

CVE 編號	CVE-2025-59470
影響產品	Veeam Backup & Replication
解決辦法	更新 Veeam Backup & Replication 至 13.0.1.1071(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-2025-59470，CVSS：9.0)允許 Backup 或 Tape Operator 傳送惡意 interval 或 order 參數，以 postgres 使用者身分執行遠端程式碼(RCE)。

- 影響平台：
  - Veeam Backup & Replication 13.0.1.180 (含)之前 13 版本
- 資料來源：
  1. Vulnerabilities Resolved in Veeam Backup & Replication 13.0.1.1071

2.2.4 趨勢科技旗下 Trend Micro Apex Central 存在重大資安漏洞(CVE-2025-69258)

CVE 編號	CVE-2025-69258
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-0022071

- 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。近日發布重大資安漏洞公告，此漏洞(CVE-2025-69258，CVSS：9.8)為 Trend Micro Apex Central 使用的 LoadLibraryEX 函式存在安全弱點，攻擊者可在未經身分驗證的情況下，遠端將其控制的惡意 DLL 載入系統中的關鍵執行檔，並以 SYSTEM 權限執行攻擊者的程式碼。

- 影響平台：
  - Apex Central (on-premise) 7190 (不含)之前版本
- 資料來源：
  1. CRITICAL SECURITY BULLETIN: Trend Micro Apex Central (on-premise) January 2026
  2. CVE-2025-69258

2.2.5 QNAP NAS應用程式存在高風險安全漏洞(CVE-2025-59384與CVE-2025-59387)

CVE 編號	CVE-2025-59384,CVE-2025-59387
影響產品	QNAP NAS 應用程式
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.qnap.com/en/security-advisory/qsa-25-54 https://www.qnap.com/en/security-advisory/qsa-25-53

- 內容說明：

  研究人員發現 QNAP NAS 應用程式存在高風險安全漏洞，請儘速確認並進行修補。

  1. Qfiling 存在路徑遍歷(Path Traversal)漏洞(CVE-2025-59384)，未經身分鑑別之遠端攻擊者可利用此漏洞讀取未授權之檔案或系統資料。
  2. MARS(Multi-Application Recovery Service)存在 SQL 注入(SQL Injection)漏洞(CVE-2025-59387)，未經身分鑑別之遠端攻擊者可注入並執行未授權指令。

- 影響平台：
  - Qfiling 3.13.x 至 3.13.1(不含)版本
  - MARS 1.2.x 至 1.2.1.1686(不含)版本

- 資料來源：
  1. CVE-2025-59384
  2. CVE-2025-59387
  3. Vulnerability in Qfiling
  4. Vulnerability in MARS (Multi-Application Recovery Service)

2.2.6 Fortinet旗下 FortiFone Web Portal 存在重大資安漏洞(CVE-2025-47855)

CVE 編號	CVE-2025-47855
影響產品	Fortinet FortiFone Web Portal
解決辦法	請更新至以下版本： FortiFone 3.0.24(含)之後版本 FortiFone 7.0.2(含)之後版本

- 內容說明：

  FortiFone Web Portal 是 Fortinet FortiVoice 系統的集中管理介面，用於遠端配置電話分機、監控通話紀錄與系統效能。日前，Fortinet 發布重大資安漏洞公告，此漏洞(CVE-2025-47855，CVSS：9.8)可能允許未經身分驗證的攻擊者，透過精心設計的 HTTP 或 HTTPS 請求取得裝置配置，從而取得敏感資料。

- 影響平台：
  - FortiFone 3.0.13 至 3.0.23 版本
  - FortiFone 7.0.0 至 7.0.1 版本
- 資料來源：
  1. Unauthenticated access to local configuration
  2. CVE-2025-47855

2.2.7 Fortinet旗下FortiSIEM存在重大資安漏洞(CVE-2025-64155)

CVE 編號	CVE-2025-64155
影響產品	Fortinet FortiSIEM
解決辦法	請更新至以下版本： FortiSIEM 7.1.9(含)之後版本 FortiSIEM 7.2.7(含)之後版本 FortiSIEM 7.3.5(含)之後版本 FortiSIEM 7.4.1(含)之後版本 備註：FortiSIEM 6.7 和 FortiSIEM 7.0 版本請遷移至固定版本

- 內容說明：

  FortiSIEM 是 Fortinet 旗下的次世代安全資訊與事件管理平台，運用 AI 和自動化技術，提升威脅偵測與安全營運效率，降低管理複雜度。近日，Fortinet 發布重大資安漏洞公告(CVE-2025-64155，CVSS：9.8)，此為作業系統指令注入漏洞，可能允許未經身分驗證的攻擊者，透過特製的 TCP 請求，執行未經授權的程式碼或命令。

- 影響平台：
  - FortiSIEM 6.7.0 至 6.7.10 版本
  - FortiSIEM 7.0.0 至 7.0.4 版本
  - FortiSIEM 7.1.0 至 7.1.8 版本
  - FortiSIEM 7.2.0 至 7.2.6 版本
  - FortiSIEM 7.3.0 至 7.3.4 版本
  - FortiSIEM 7.4.0 版本
- 資料來源：
  1. Unauthenticated remote command injection
  2. CVE-2025-64155

2.2.8 Microsoft 旗下SharePoint Server 存在2個重大資安漏洞

CVE 編號	CVE-2026-20947,CVE-2026-20963
影響產品	Microsoft SharePoint Server
解決辦法	根據官方網站釋出解決方式進行修補： 【CVE-2026-20947】 https://msrc.microsoft.com/update-guide/zh-tw/vulnerability/CVE-2026-20947 【CVE-2026-20963】 https://msrc.microsoft.com/update-guide/zh-tw/vulnerability/CVE-2026-20963

- 內容說明：

  Microsoft SharePoint Server 是一款企業級協作平台，提供文件管理與團隊協作等功能，是企業資訊整合的核心平台。近期微軟發布重大資安公告(CVE-2026-20947，CVSS：8.8 和 CVE-2026-20963，CVSS：8.8)，CVE-2026-20947 為 SQL 注入漏洞，經授權的攻擊者可透過網路執行任意 SQL 命令；CVE-2026-20963 為不受信任資料之反序列化漏洞，允許經授權的攻擊者透過網路執行任意程式碼。

- 影響平台：
  - Microsoft SharePoint Server Subion Editio
  - Microsoft SharePoint Server 2019
  - Microsoft SharePoint Enterprise Server 2016
- 資料來源：
  1. Microsoft SharePoint Server 遠端執行程式碼弱點
  2. Microsoft SharePoint 遠端執行程式碼弱點
  3. CVE-2026-20947
  4. CVE-2026-20963

2.2.9 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2026-0491,CVE-2026-0492,CVE-2026-0498,CVE-2026-0500,CVE-2026-0501
影響產品	SAP S/4HANA、Wily Introscope Enterprise Manager、 Landscape Transformation
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/january-2026.html

- 內容說明：

【CVE-2026-0501，CVSS：9.9】

此漏洞存在於 SAP S/4HANA 私有雲和本地部署(Financials – General Ledger)，由於輸入驗證不足，允許經過身分驗證的攻擊者利用特製的 SQL 指令進行讀取、修改和刪除後端資料庫資料。

【CVE-2026-0500，CVSS：9.6】

由於 SAP Wily Introscope Enterprise Manager (WorkStation)使用易受攻擊的第三方元件，未經身分驗證的攻擊者可建立公開 URL 存取的惡意 JNLP 文件，導致受害者點擊 URL 時，Wily Introscope 伺服器可在受害者電腦上執行作業系統命令。

【CVE-2026-0498，CVSS：9.1】

此漏洞存在於 SAP S/4HANA 的私有雲和本地部署，允許具有管理員權限的攻擊者透過 RFC 公開功能模組的漏洞，將任意 ABAP 程式碼/作業系統命令注入系統，從而繞過必要的授權檢查。

【CVE-2026-0491，CVSS：9.1】

SAP Landscape Transformation 允許擁有管理員權限的攻擊者利用 RFC 公開函數模組漏洞，將任意 ABAP 程式碼/作業系統命令注入系統，從而繞過必要的授權檢查。

【CVE-2026-0492，CVSS：8.8】

SAP HANA 資料庫存在權限提升漏洞，允許攻擊者擁有使用者的有效憑證，即可切換其他用戶，從而獲得管理員權限。

- 影響平台：

【CVE-2026-0501】

- SAP S/4HANA Private Cloud and On-Premise (Financials – General Ledger) S4CORE 102, 103, 104, 105, 106, 107, 108, 109 版本

【CVE-2026-0500】

- SAP Wily Introscope Enterprise Manager (WorkStation) WILY_INTRO_ENTERPRISE 10.8 版本

【CVE-2026-0498】

- SAP S/4HANA (Private Cloud and On-Premise) S4CORE 102, 103, 104, 105, 106, 107, 108, 109 版本

【CVE-2026-0491】

- SAP Landscape Transformation DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2018_1_752, 2020 版本

【CVE-2026-0492】

- SAP HANA database HDB 2.00 版本

- 資料來源：

1. SAP Security Patch Day - January 2026
2. CVE-2026-0501
3. CVE-2026-0500
4. CVE-2026-0498
5. CVE-2026-0491
6. CVE-2026-0492

2.2.10 HPE 旗下OneView存在重大資安漏洞(CVE-2025-37164)

CVE 編號	CVE-2025-37164
影響產品	HPE OneView
解決辦法	根據官方網站釋出的解決方式進行修補： https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US#resolution-4

- 內容說明：

  HPE OneView 是一款 IT 基礎設施管理平台解決方案，利用自動化控制伺服器、儲存與網路，簡化管理並提升效率。近期 HPE 發布重大資安公告(CVE-2025-37164，CVSS：10.0)，此為程式碼注入漏洞，允許未經身分驗證的遠端攻擊者可利用此漏洞於受影響設備執行任意程式碼。

  備註：目前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：
  - HPE OneView v10.20(含)以前所有版本
- 資料來源：
  1. HPE-Support Center
  2. CVE-2025-37164

2.2.11 n8n存在4個重大資安漏洞

CVE 編號	CVE-2025-68613,CVE-2025-68668,CVE-2026-21877,CVE-2026-21858
影響產品	n8n
解決辦法	【CVE-2025-68613】 請更新至以下版本： n8n 1.120.4 版本、1.121.1 版本、1.122.0 版本 【CVE-2025-68668】 請更新至以下版本： n8n 2.0.0 版本 【CVE-2026-21877】 請更新至以下版本： n8n 1.121.3 版本 【CVE-2026-21858】 請更新至以下版本： n8n 1.121.0 版本

- 內容說明：

  n8n 是一款開源工作流程自動化工具，透過視覺化拖拉介面串接多種應用程式，無需程式碼即可自動化重複性任務。近期 n8n 發布多個重大資安漏洞公告。

  【CVE-2025-68613，CVSS：9.9】

  此為遠端程式碼執行漏洞，在特定條件下，允許經身分驗證的攻擊者以 n8n 行程的權限執行任意程式碼。

  【CVE-2025-68668，CVSS：9.9】

由於 n8n 使用 Pyodide 的 Python 程式碼節點存在沙箱繞過漏洞，經身分驗證且具有建立或修改工作流程權限的攻擊者，以 n8n 行程相同權限在 n8n 伺服器上執行任意命令。

【CVE-2026-21877，CVSS：10.0】

此漏洞允許經過身分驗證的攻擊者，可利用 n8n 服務執行惡意程式碼，導致系統完全被破壞。

【CVE-2026-21858，CVSS：10.0】

此漏洞允許未經身分驗證的攻擊者，可透過執行某些基於表單工作流程，存取底層伺服器的檔案，導致儲存在系統中的敏感資料外洩。

- 影響平台：

【CVE-2025-68613】

- n8n 0.211.0 至 1.120.4(不含)之前版本
- n8n 1.121.0 版本

【CVE-2025-68668】

- n8n 1.0.0 至 2.0.0(不含)之前版本

【CVE-2026-21877】

- n8n 0.121.2 (含)之前版本

【CVE-2026-21858】

- n8n 1.65.0 至 1.121.0(不含)之前版本

- 資料來源：

1. n8n-security
2. CVE-2025-68613
3. CVE-2025-68668
4. CVE-2025-21877
5. CVE-2025-21858

2.2.12 Zoom Node 多媒體路由器存在重大資安漏洞(CVE-2026-22844)

CVE 編號	CVE-2026-22844
影響產品	Zoom Node Multimedia Routers
解決辦法	根據官方網站釋出的解決方式進行修補： https://www.zoom.com/en/trust/security-bulletin/zsb-26001/

- 內容說明：

  Zoom Node Multimedia Routers (MMRs) 是由 Zoom 所提供的混合雲端解決方案核心模組，主要用於處理會議媒體流量、提升頻寬效率和降低延遲等需求。近日 Zoom 發布重大資安公告(CVE-2026-22844，CVSS：9.9)，此為命令注入漏洞，會議參與者可能透過網路存取對 MMRs 執行遠端程式碼。

- 影響平台：
  - Zoom Node Meetings Hybrid (ZMH) MMR module 5.2.1716.0(不含)以前版本
  - Zoom Node Meeting Connector (MC) MMR module 5.2.1716.0(不含)以前版本
- 資料來源：
  1. Zoom Node Deployments - Command Injection
  2. CVE-2026-22844

2.2.13 Oracle針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2026-21962,CVE-2026-21969
影響產品	Oracle Fusion Middleware、Supply Chain
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/cpujan2026.html

- 內容說明：

  【CVE-2026-21962，CVSS：10.0】

  此漏洞存在 Oracle Fusion Middleware 的 Oracle HTTP Server 與 Oracle Weblogic Server Proxy Plug-in 產品中。允許未經身分驗證的攻擊者透過 HTTP 存取相關服務，若攻擊者成功利用，可能導致未經授權的敏感資料建立、刪除、修改和存取。

  【CVE-2026-21969，CVSS：9.8】

  此漏洞存在 Oracle Supply Chain 的 Oracle Agile Product Lifecycle Management for Process 產品中。允許未經身分驗證的攻擊者透過 HTTP 存取入侵系統，進而造成系統遭完全接管。

- 影響平台：

  【CVE-2026-21962】

  - Oracle Fusion Middleware 12.2.1.4.0
  - Oracle Fusion Middleware 14.1.1.0.0
  - Oracle Fusion Middleware 14.1.2.0.0

  【CVE-2026-21969】

  - Oracle Supply Chain 6.2.4

- 資料來源：

  1. Oracle Critical Patch Update Advisory - January 2026
  2. CVE-2026-21962
  3. CVE-2026-21969

2.2.14 Fortinet 的 FortiCloud SSO 存在重大資安漏洞(CVE-2026-24858)

CVE 編號	CVE-2026-24858
影響產品	Fortinet FortiAnalyzer、FortiManager、FortiOS、FortiProxy
解決辦法	請更新至以下版本： FortiAnalyzer 7.6.6(含)之後版本 FortiAnalyzer 7.4.10(含)之後版本 FortiAnalyzer 7.2.12(含)之後版本 FortiAnalyzer 7.0.16(含)之後版本 FortiManager 7.6.6(含)之後版本 FortiManager 7.4.10(含)之後版本 FortiManager 7.2.13(含)之後版本 FortiManager 7.0.16(含)之後版本 FortiOS 7.6.6(含)之後版本 FortiOS 7.4.11(含)之後版本 FortiOS 7.2.13(含)之後版本 FortiOS 7.0.19(含)之後版本 FortiProxy 7.6.6(含)之後版本 FortiProxy 7.4.13(含)之後版本 備註：FortiProxy 7.2 和 FortiProxy 7.0 請遷移至固定版本

- 內容說明：

  Fortinet 針對 FortiCloud SSO 發布重大資安漏洞公告(CVE-2026-24858，CVSS：9.8)，此為身分驗證繞過漏洞，允許擁有 FortiCloud 帳號和已註冊設備的攻擊者，登入註冊到其他帳號的其他設備。

  備註：目前 Fortinet 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：
  - FortiAnalyzer 7.6.0 至 7.6.5 版本
  - FortiAnalyzer 7.4.0 至 7.4.9 版本
  - FortiAnalyzer 7.2.0 至 7.2.11 版本
  - FortiAnalyzer 7.0.0 至 7.0.15 版本
  - FortiManager 7.6.0 至 7.6.5 版本
  - FortiManager 7.4.0 至 7.4.9 版本
  - FortiManager 7.2.0 至 7.2.11 版本
  - FortiManager 7.0.0 至 7.0.15 版本
  - FortiOS 7.6.0 至 7.6.5 版本
  - FortiOS 7.4.0 至 7.4.10 版本
  - FortiOS 7.2.0 至 7.2.12 版本
  - FortiOS 7.0.0 至 7.0.18 版本
  - FortiProxy 7.6.0 至 7.6.4 版本
  - FortiProxy 7.4.0 至 7.4.12 版本
  - FortiProxy 7.2 所有版本
  - FortiProxy 7.0 所有版本
- 資料來源：
  1. Administrative FortiCloud SSO authentication bypass
  2. CVE-2026-24858

2.2.15 Cisco整合通訊多項產品存在重大資安漏洞(CVE-2026-20045)

CVE 編號	CVE-2026-20045
影響產品	Cisco Unity Connection、Unified CM、Unified CM SME、Unified CM IM&P、Webex Calling Dedicated Instance
解決辦法	根據官方網站釋出的解決方式進行修補： https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

- 內容說明：

  Cisco 針對旗下多項整合通訊產品發布重大資安漏洞公告(CVE-2026-20045，CVSS：8.2)，此漏洞為 HTTP 請求驗證不當，未經身分驗證的遠端攻擊者可能透過特製的 HTTP 請求至受影響設備，以執行任意指令，進而提升 root 權限。

  備註：目前 Cisco 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：

  以下產品 12.5、14 及 15 版本：

  - Unity Connection
  - Unified Communications Manager(Unified CM)
  - Unified CM Session Management Edition(Unified CM SME)
  - Unified CM IM & Presence Service(Unified CM IM&P)
  - Webex Calling Dedicated Instance

- 資料來源：

  1. Cisco Unified Communications Products Remote Code Execution Vulnerability
  2. CVE-2026-20045

2.2.16 SolarWinds旗下Web Help Desk (WHD)存在4個重大資安漏洞

CVE 編號	CVE-2025-40551,CVE-2025-40552,CVE-2025-40553,CVE-2025-40554
影響產品	SolarWinds Web Help Desk
解決辦法	根據官方網站釋出的解決方式進行修補： https://documentation.solarwinds.com/en/success_center/whd/content/release_notes/whd_2026-1_release_notes.htm

- 內容說明：

  Web Help Desk (WHD)是 SolarWinds 旗下產品，主要提供集中式自動執行工單管理的服務，包含工單自動化、集中式知識庫、資產追蹤管理等，以便支援客戶與追蹤事項，近日發布重大資安漏洞公告。

  【CVE-2025-40551，CVSS：9.8】

  此為不受信任資料反序列化漏洞，允許未經身分驗證的攻擊者可在主機上執行命令，可能導致遠端程式碼執行。

  【CVE-2025-40552，CVSS：9.8】

  此為身分驗證繞過漏洞，若攻擊者利用該漏洞，可執行本應受身分驗證保護的相關服務。

  【CVE-2025-40553，CVSS：9.8】

  此為不受信任資料反序列化漏洞，允許未經身分驗證的攻擊者可在主機上執行命令，可能導致遠端程式碼執行。

  【CVE-2025-40554，CVSS：9.8】

  此為身分驗證繞過漏洞，若攻擊者利用該漏洞，可在 Web Help Desk(WHD)中執行特定操作。

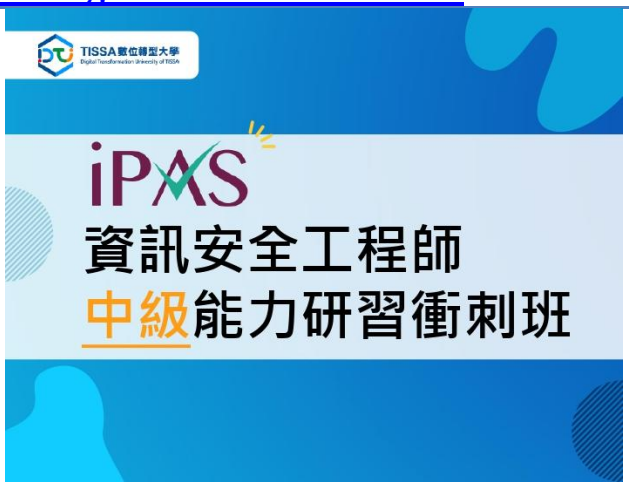
- 影響平台：
  - SolarWinds Web Help Desk (WHD) 12.8.8 HF1(含)以下版本

- 資料來源：
  1. WHD 2026.1 release notes
  2. CVE-2025-40551
  3. CVE-2025-40552
  4. CVE-2025-40553
  5. CVE-2025-40554

第 3 章、資安研討會及活動

- **資安研討會**

【資安學院】115/1/30-資通系統委外開發RFP全攻略—SSDLC及安全程式設計	
活動時間	**115/1/30 14:00 ~ 17:00**
活動地點	**中華軟體公會—大同辦公室D01會議室（ 臺北市中山北路三段22-1號新設工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5873**
活動概要	 **【費用】** 原價：4,000元/人 早鳥價：3,800元/人 公會會員價：3,500元/人 費用含稅、教材及完課證明 報名截止： 2026/01/28 **【活動內容 / Event Deails】** 本課程旨在針對委外開發技術面及管理面資安需求，並依據資通系統防護基準控制措施構面，進行 SSDLC 安全的系統開發生命週期實

	務操作，制定資安需求項目資訊系統委外安全管理。 課程內容將深度探討 ISO/IEC 27001:2022 附錄 A.8.2.5 (安全開發生命週期) 與 SSDLC 實務的實質關聯性與對應關係，並細分為以下三個關鍵階段進行教學與：針對安全需求定義、安全設計與開發、安全部署與維護。 **【主辦單位】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**
【資安學院】115/3/5~3/6-iPAS-「中級」資訊安全工程師-能力研習衝刺班	
活動時間	**2026-03-05 09:00 ~ 2026-03-06 16:00**
活動地點	**中華軟體公會──大同辦公室D01會議室（臺北市中山北路三段22-1號新設工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5881**
活動概要	 **【費用】** 原價：12,000元/人 早鳥價：11,000元/人 軟協會員：9,000元/人 費用含稅、教材、餐點及完課證明 報名截止： 2026-03-02

	【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】中華民國資訊軟體服務商業同業公會** **【聯絡窗口】02-2553-3988#816 林專員** **security@tissa.org.tw**

【資安學院】115/3/18-個資守門員：從法規遵循、風險處理到事故應變	
活動時間	**2026-03-18 14:00 ~ 2026-03-18 17:00**
活動地點	**中華軟體公會──大同辦公室D01會議室（臺北市中山北路三段22-1號新設工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5880**
活動概要	 **【費用】** 原價：4,000元/人 早鳥價：3,800元/人 軟協會員：3,500元/人 費用含稅、教材及完課證明 報名截止： 2026-03-16

	【活動內容 / Event Deails】 近年來個資外洩事故頻傳，個資保護成為政府及企業當前重要課題，因此個資法分別於 112 年 5 月 16 日及 114 年 10 月 17 日進行修正，並經立院三讀通過，調高未適當保護個資之罰則最高重罰 1,500 萬元，並要求業者知悉個資事故時應於 72 小時內通報主管機關，未通報者教可能被裁罰最高 20 萬元。 本課程將講述個資法之安全維護概念及實務操作，說明個資安維措施制度之核心內容，並透過分組討論、案例探討，教導您如何進行個資盤點及風險評估，做好採取適當個資安危措施之第一步。此外，課程中亦說明個資外洩處理流程，當不幸發生個資外洩事故時，能夠第一時間了解事故發生原因，進行緊急應變措施控制事故狀況，避免風險繼續擴大。 **【主辦單位】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**
【資安學院】115/3/25-從零到認證—ISO 27001導入步驟及重點前導課程	
活動時間	**2026-03-25 09:00 ~ 16:00**
活動地點	**中華軟體公會—大同辦公室D01會議室（臺北市中山北路三段22-1號新設工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5874**
活動概要	

	【費用】 原價：7,200元/人 早鳥價：6,800元/人 軟協會員：6,000元/人 費用含稅、教材、餐點及完課證明 報名截止： 2026-03-20 **【活動內容 / Event Deails】** 本課程旨在使學員深入瞭解國際資訊安全管理系統標準 ISO 27001:2022 及相關法規要求之重點內容，課程涵蓋 ISO 27001:2022 標準架構、資安目標之訂定、風險管理流程、各項控制措施，以及資訊管理監督及稽核等內容。 課程中納入多項實務案例，透過分組討論、情境演練與案例研討等互動式教學，強化學員建置資訊安全管理系統的實務能力，利於企業在未來導入 ISO 27001:2022，以期持續提升組織整體資安環境。 **【主辦單位】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**

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：

廣達電腦｜QOCA aim AI醫療雲平台 - Arbitrary File Upload	
TVN / CVE ID	TVN-202601001 / CVE-2025-15240
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	QOCA aim v2.7.5(含)以前版本
問題描述	QOCA aim AI醫療雲平台存在Arbitrary File Upload漏洞，已通過身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼。
解決方法	請更新至v2.7.6(含)以後版本
公開日期	2026-01-05
相關連結	https://www.twcert.org.tw/tw/cp-132-10615-157a3-1.html
利凌｜監控主機 - OS Command Injection	
TVN / CVE ID	TVN-202601003 / CVE-2026-0854
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	影響型號與韌體版本： DH032：v1.0.28.3858(含)以前版本 DVR708, DVR716：v1.3.4(含)以前版本 DVR804, DVR808, DVR816：v1.3.4(含)以前版本 NVR100L, NVR200L, NVR400L, NVR1400L, NVR2400L：v1.1.66(含)以前版本 NVR3216, NVR3416, NVR3416r, NVR3816：v2.0.74.3921(含)

	以前版本 NVR5832, NVR5832S：v4.0.24.4043(含)以前版本 NVR5104E, NVR5208E, NVR5416E：v4.0.24.4078(含)以前版本
問題描述	利凌開發之部分監控主機型號存在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設備上執行。
解決方法	請參考官方公告(M00175)進行韌體版本更新
公開日期	2026-01-12
相關連結	**https://www.twcert.org.tw/tw/cp-132-10624-6599c-1.html**
利凌｜監控攝影機 - OS Command Injection	
TVN / CVE ID	TVN-202601004 / CVE-2026-0855
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	監控攝影機P2/ P3/ Z7/ P6/ V1/ IPD/ IPR/ LD/ LR系列型號
問題描述	利凌開發之部分監控攝影機型號存在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設備上執行。
解決方法	IPD/IPR/LD/LR機種已停止支援，建議進行更換，其餘受影響機種請參考官方公告(M00176)進行韌體版本更新
公開日期	2026-01-12
相關連結	**https://www.twcert.org.tw/tw/cp-132-10625-fac5c-1.html**
金諄資訊｜警政統計資料庫系統 - 存在2個漏洞	
TVN / CVE ID	TVN-202601005 / CVE-2026-1019, CVE-2026-1021
CVSS	CVE-2026-1019：

	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVE-2026-1021： 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	警政統計資料庫系統1.0.2(含)以前版本
問題描述	CVE-2026-1019： 警政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利用特定功能讀取、修改及刪除資料庫內容。 CVE-2026-1021： 警政統計資料庫系統存在Arbitrary File Upload漏洞，未經身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼。
解決方法	更新至1.0.3(含)以後版本
公開日期	2026-01-16
相關連結	**https://www.twcert.org.tw/tw/cp-132-10637-3e4b3-1.html**
普羅通信｜PrismX MX100 AP controller - Use of Hard-coded Credentials	
TVN / CVE ID	TVN-202601007 / CVE-2026-1221
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	PrismX MX100 AP controller v1.03.23.01(不含)以前版本
問題描述	PrismX MX100 AP controller 存在 Use of Hard-coded Credentials漏洞，未經身分鑑別之遠端攻擊者可利用寫入於韌體中的資料庫帳號與通行碼登入資料庫。
解決方法	請更新韌體至v1.03.23.01(含)以後版本
公開日期	2026-01-20

相關連結	https://www.twcert.org.tw/tw/cp-132-10642-3b808-1.html
哈瑪星科技｜MeetingHub 無紙化會議 - Arbitrary File Upload	
TVN / CVE ID	TVN-202601008 / CVE-2026-1331
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	MeetingHub(需安裝簽到退模組)
問題描述	MeetingHub無紙化會議存在Arbitrary File Upload漏洞，未經身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼。
解決方法	安裝修補程式20251210(含)以後版本
公開日期	2026-01-22
相關連結	https://www.twcert.org.tw/tw/cp-132-10650-a5ee9-1.html
銘祥科技實業｜多合一室內空氣品質監測器（IAQS）與觸控型7吋IoT預警控制系統（I6）- 存在2個漏洞	
TVN / CVE ID	TVN-202601009 / CVE-2026-1363, CVE-2026-1364
CVSS	CVE-2026-1363： 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVE-2026-1364： 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	多合一室內空氣品質監測器（IAQS）與觸控型7吋IoT預警控制系統（I6）
問題描述	CVE-2026-1363： 多合一室內空氣品質監測器（IAQS）與觸控型7吋IoT預警控制系統（I6）存在Client-Side Enforcement of Server-Side Security漏洞，未經身分鑑別之遠端攻擊者可透過調

	整網頁前端取得管理者權限。 CVE-2026-1364： 多合一室內空氣品質監測器（IAQS）與觸控型7吋IoT預警控制系統（I6）存在Missing Authentication漏洞，未經身分鑑別之遠端攻擊者可直接操作系統管理功能。
解決方法	廠商已針對使用M4晶片之設備釋出修補，使用M3晶片之設備不支援更新，建議進行更換。請聯繫廠商確認設備使用之晶片並採取對應措施。
公開日期	2026-01-23
相關連結	https://www.twcert.org.tw/tw/cp-132-10652-4cdca-1.html
葳橋資訊｜單一簽入暨電子目錄服務系統 - 存在2個漏洞	
TVN / CVE ID	TVN-202601010 / CVE-2026-1427, CVE-2026-1428
CVSS	CVE-2026-1427： 8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CVE-2026-1428： 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	電子目錄服務系統(V4) IFTOP_P4_181(不含)以前版本
問題描述	CVE-2026-1427： 單一簽入暨電子目錄服務系統存在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。 CVE-2026-1428： 單一簽入暨電子目錄服務系統存在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	更新電子目錄服務系統(V4)至IFTOP_P4_181以上
公開日期	2025-12-29
相關連結	**https://www.twcert.org.tw/tw/cp-132-10654-23f40-1.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1月31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/**