TWCERT/CC 資安情資電子報

2026 年 2 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

CISA發布警告：間諜軟體向即時通訊應用程式用戶發動攻擊

美國網路安全和基礎設施安全局(CISA)針對不斷升級的網路間諜活動發布警報《Spyware Allows Cyber Threat Actors to Target Users of Messaging Applications》並更新行動通訊最佳實作《Mobile Communications Best Practice Guidance》。鑑於針對行動通訊軟體的攻擊數量和複雜度持續增加，呼籲所有使用者提高警覺，以應對不斷升級的網路間諜活動。

CISA指出多個網路攻擊者，正積極利用商業間諜軟體，鎖定即時通訊應用程式的使用者。這些攻擊者透過高度複雜的目標鎖定手法與社

交工程技術部署間諜軟體，從而未經授權存取受害者資料，並進一步植入惡意程式，危害行動裝置的安全。目前CISA觀察到攻擊者主要使用的策略包含：

1. 帳戶盜用：透過網路釣魚和惡意QR Code誘導用戶將帳戶連結到攻擊者控制設備。
2. 零點擊漏洞（Zero-click exploits）攻擊：此類攻擊無需使用者採取任何行動，攻擊者即可在設備中植入惡意軟體。
3. 偽裝應用程式：偽冒Signal、WhatsApp等知名通訊應用程式，誘騙使用者下載含有惡意程式碼的偽冒版本。

為協助使用者抵禦惡意威脅，新版指南強化保護端點與加密通訊的防護措施，CISA所提出的關鍵安全措施包含：

一、行動通訊安全最佳實務

1. 落實端對端加密(E2EE)：僅使用具備端對端加密技術的通訊工具，確保訊息在傳輸過程中無法被攔截與解密。
2. 謹慎評估應用程式隱私政策：選擇通訊軟體時，務必檢視該應用程式及其相關服務對資料收集的範圍與內容。
3. 優先採用高安全性平台：建議使用預設提供 E2EE 的即時通訊應用程式。
4. 對系統警示保持高度警戒：特別是要求「重新驗證身分」或「連結新裝置」的提示，這往往是攻擊者試圖劫持帳號的常見手法。

二、強化身分驗證機制

1. 導入防釣魚的多因子驗證(MFA)：啟用基於FIDO標準的 MFA

機制。

2. 優先採用實體安全金鑰：強烈建議使用硬體型FIDO安全金鑰(如Yubico 或 Google Titan)，FIDO密碼密鑰(Passkey)亦為可接受的替代方案。
3. 限縮核心帳號驗證途徑：針對 Microsoft、Apple 和 Google 等核心帳戶，在啟用硬體金鑰後，應主動停用其他安全性較低的 MFA 形式。

三、停用簡訊(SMS)雙重驗證

1. 避免使用SMS作為第二因子驗證：由於簡訊傳輸並未加密，攻擊者可輕易攔截、讀取驗證碼，或透過SIM卡交換攻擊(SIM Swapping)進行竊取。
2. 移除舊有弱點：在帳戶註冊了更安全的身分驗證器或 FIDO MFA 後，應立即至設定中「停用」SMS 驗證，避免其成為攻擊者降級攻擊的破口。

更多詳細建議可參考《Mobile Communications Best Practice Guidance》，其中亦提供針對iPhone與Android使用者的特定安全強化措施。

- 相關連結
  1. Spyware Allows Cyber Threat Actors to Target Users of Messaging Applications
  2. Mobile Communications Best Practice Guidance

第 2 章、國內外重要資安事件

2.1 國際政府組織資安資訊

2.1.1 ETSI發布EN 304 223標準，強化人工智慧模型與系統資安防護

歐洲電信標準協會(ETSI)近日正式發布ETSI EN 304 223 標準，為人工智慧（AI）模型與系統建立全球通用的資安基準。該標準獲歐洲各國國家標準組織投票通過，具高度權威性與國際適用性，被視為AI資安治理的重要里程碑。

隨著 AI 技術廣泛導入關鍵服務與產業場域，傳統資安防護已不足以因應新型威脅。ETSI 指出，AI 系統的風險不僅源自程式本身，更涵蓋資料管線、模型行為與營運環境，例如資料毒化、模型混淆、間接提

示注入，以及複雜訓練與部署流程所衍生的潛在弱點，皆對組織資安形成新挑戰。

ETSI EN 304 223 採全生命週期方法，於安全設計、開發、部署、維護及終止營運五大階段中，定義 13 項核心原則與要求，並與國際公認的 AI 生命週期模型對齊，確保與既有標準與指引的相容性與互通性，協助資安團隊在 AI 系統整體營運過程中落實防護。

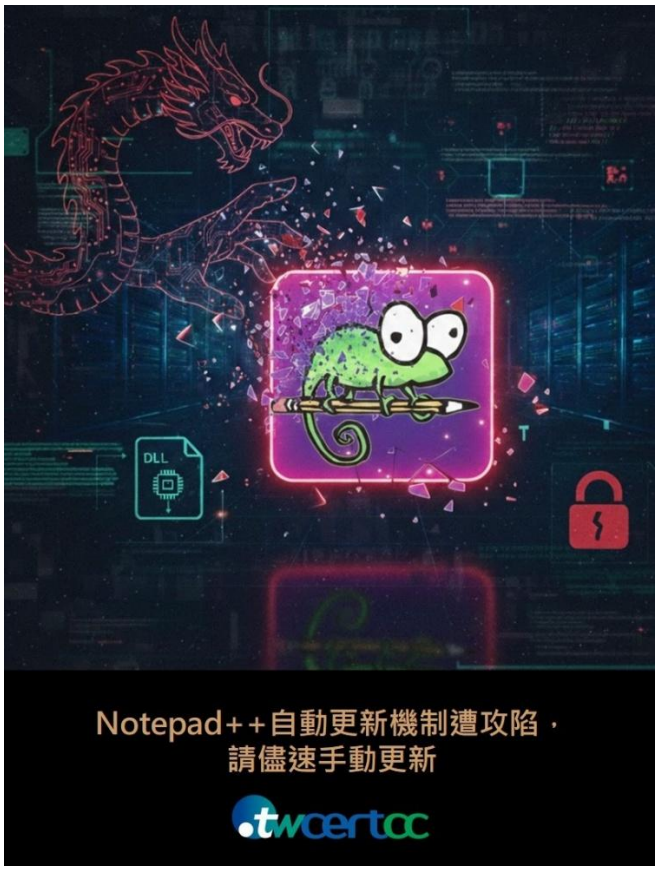
值得注意的是，該標準適用於採用深度神經網路(如生成式AI)，且實際部署於營運環境的 AI 系統，並明確排除了僅供學術研究用途的系統。此外，標準明確劃分了 AI 供應鏈中各方利害關係人的資安責任，包含開發者（Developers）、系統營運商（System Operators）、資料保管者（Data Custodians）以及終端使用者（End-users），藉此作為供應商與系統整合商的共同依據，強化跨組織與跨產業的資安治理能力。

整體而言，ETSI EN 304 223 為 AI 系統安全奠定一致且嚴謹的基礎。在 AI 日益融入關鍵基礎設施與核心服務的趨勢下，該標準提供清晰且可落實的資安指引，有助於提升 AI 系統的韌性與可信度，落實「安全即設計」（secure by design），並成為未來 AI 資安治理與合規的重要參考。

- 相關連結
  1. ETSI releases world-leading standard for securing AI
  2. ETSI EN 304 223 - Securing Artificial Intelligence (SAI)

2.2 軟硬體系統資安議題

2.2.1 Notepad++自動更新機制遭攻陷，請儘速手動更新



近期資安研究團隊Rapid7 Labs與Rapid7 MDR聯合揭露一場針對知名開源文字編輯器「Notepad++」的複雜供應鏈攻擊。此攻擊由中國APT組織Lotus Blossom(亦被追蹤為Violet Typhoon 或 Billbug)發起。攻擊者於2025年6 月至12月期間，成功攻陷Notepad++代管主機服務商的基礎設施。與傳統竄改軟體原始碼的手法不同，攻擊者係掌控了內部服務憑證，導致使用者執行內建更新程式(WinGUp)時，流量會被導向惡意伺服器並下載偽造的安裝套件。官方已緊急呼籲所有用戶立即停止使用自動更新功能，並務必透過官方網站手動下載安裝最新的v8.9.2版本。

透過本次攻擊活動顯示威脅行為者具高度的技術與規避偵測能力，

攻擊鏈始於惡意的NSIS安裝檔(update.exe)，利用DLL側載(DLL Sideloading)技術，透過合法的Bitdefender執行檔(被重新命名為BluetoothService.exe)載入惡意元件log.dll，進而解密並執行Shellcode，最終植入名為「Chrysalis」的客製化隱匿後門。惡意NSIS安裝檔(updata.exe)執行流程如圖1所示。

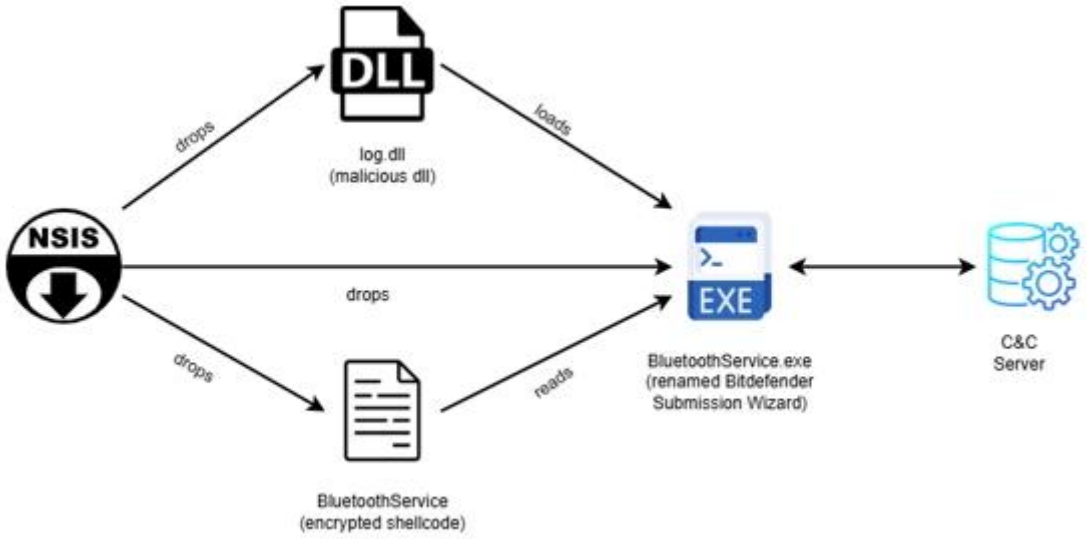


圖1：updata.exe執行流程圖。圖片來源： Rapid7

為規避EDR(端點偵測與回應)與網路流量分析，後門程式Chrysalis 採用多層次的防禦技術：

1. **C2通訊偽裝**：透過HTTPS傳輸，其URL結構(如 /a/chat/s/{GUID})刻意模仿Deepseek API端點，並搭配合法的Chrome User Agent與RC4 內容加密，使其流量在視覺與內容上皆隱匿於正常的AI應用與網頁瀏覽流量中。
2. **API Hashing**：實現雙層防禦機制。載入器階段結合FNV-1a與MurmurHash演算法；主模組則進階採用自定義的多階段算術混合運算。這種動態解析Windows API的手法，大幅提升靜態分析與特徵碼偵測的難度。

3. **濫用 Microsoft Warbird**：研究人員發現其載入器(Loader)濫用了微軟未公開的 Warbird 程式碼保護框架，透過 NtQuerySystemInformation 系統調用中的 SystemCodeFlowTransition(0xB9)類別，在合法的微軟簽章檔(clipc.dll)記憶體空間內執行惡意Shellcode。

此外，卡巴斯基資安研究團隊發現，針對此次攻擊共有3種攻擊模式：

攻擊鏈	時間範圍	惡意資源/下載位置	主要行為/目的	特色或重點
第一個攻擊鏈	2025.07~2025.08	http://45.76.155[.]202/update/update.exe	● 執行後建立「%appdata%\ProShow」資料夾 ● 收集系統資訊（whoami、tasklist 等）並上傳 ● 放置多個執行檔並執行其中惡意程式	● 視為較早期的惡意活動樣本 ● 使用舊有漏洞載入 payload
第二個攻擊鏈	2025.09	http://45.76.155[.]202/update/update.exe	● 同樣下載 update.exe ● 收集更多系統資訊（加上 systeminfo、netstat）並上傳 ● 在「%APPDATA%\Adobe\Scripts」放置多個檔案並執行惡意程式	● 資料蒐集指令更完整，範圍擴大 ● 與第一個鏈相比更新目標資料位置
第三個攻擊鏈	2025.10	http://45.32.144[.]255/update/update.exe	● 下載後置放三個檔案到「%appdata%\Bluetooth\」：「BluetoothService.exe」（合法可執行檔）、「log.dll」（惡意 DLL）、「BluetoothService」（加密 shellcode） ● 利用 DLL Hijacking 載入「log.dll」並執行後門程式 Chrysalis	● 典型 DLL Hijacking 技術 ● 最終植入後門程式（Chrysalis）

資料來源：TWCERT/CC 團隊整理

鑑於此攻擊潛伏期長且技術極其複雜，資安專家建議企業與個人用戶立即採取以下行動：

1. **立即手動修補**：確認所有端點的Notepad++ 版本已更新至 v8.9.2。請勿信任軟體跳出的自動更新提示，應直接從官方網站下載安裝。
2. **企業防禦策略強化**：透過GPO或MDM派送原則，暫時禁用非必要開源軟體自動更新功能。
3. **入侵指標(IoCs）清查**：請依據下表盤點系統環境，若發現相符項目，應立即視為受駭事件並啟動緊急應變程序。

以下是此次攻擊的入侵指標（IoCs）：

惡意IP和網域(DN)：

95[.]179[.]213[.]0
61[.]4[.]102[.]97
59[.]110[.]7[.]32
124[.]222[.]137[.]114
api[.]skycloudcenter[.]com
api[.]wiresguard[.]com

惡意檔案：

檔名	SHA-256 Hash
update.exe	a511be5164dc1122fb5a7daa3eef9467e43d8458425b15a640235796006590c9
NSIS.nsi	8ea8b83645fba6e23d48075a0d3fc73ad2ba515b4536710cda4f1f232718f53e
BluetoothService.exe	2da00de67720f5f13b17e9d985fe70f10f153da60c9ab1086fe58f069a156924
BluetoothService	77bfea78def679aa1117f569a35e8fd1542df21f7e00e27f192c907e61d63a2e
log.dll	3bdc4c0637591533f1d4198a72a33426c01f69bd2e15ceee547866f65e26b7ad
u.bat	9276594e73cda1c69b7d265b3f08dc8fa84bf2d6599086b9acc0bb3745146600

conf.c	f4d829739f2d6ba7e3ede83dad428a0ced1a703ec582fc73a4eee3df3704629a
libtcc.dll	4a52570eeaf9d27722377865df312e295a7a23c3b6eb991944c2ecd707cc9906
admin	831e1ea13a1bd405f5bda2b9d8f2265f7b1db6c668dd2165ccc8a9c4c15ea7dd
loader1	0a9b8df968df41920b6ff07785cbfebe8bda29e6b512c94a3b2a83d10014d2fd
uffhxpSy	4c2ea8193f4a5db63b897a2d3ce127cc5d89687f380b97a1d91e0c8db542e4f8
loader2	e7cd605568c38bd6e0aba31045e1633205d0598c607a855e2e1bca4cca1c6eda
3yzr31vk	078a9e5c6c787e5532a7e728720cbafee9021bfec4a30e3c2be110748d7c43c5
ConsoleApplication2.exe	b4169a831292e245ebdffedd5820584d73b129411546e7d3eccf4663d5fc5be3
system	7add554a98d3a99b319f2127688356c1283ed073a084805f14e33b4f6a6126fd
s047t5g.exe	fcc2765305bcd213b7558025b2039df2265c3e0b6401e4833123c461df2de51a

- 相關連結

1. The Chrysalis Backdoor: A Deep Dive into Lotus Blossom’s toolkit
2. Notepad++ Hack Detailed Along With the IoCs and Custom Malware Used
3. Notepad++ Official Update Mechanism Hijacked to Deliver Malware to Select Users
4. Notepad++ Hijacked by State-Sponsored Hackers
5. Notepad++ 更新基礎設施遭攻擊：疑似中國 APT 組織 Lotus Blossom 發動供應鏈滲透
6. The Notepad++ supply chain attack — unnoticed execution chains and new IoCs

2.3 軟硬體漏洞資訊

2.3.1 Ivanti旗下Endpoint Manager Mobile (EPMM)存在2個重大資安漏洞

CVE 編號	CVE-2026-1281,CVE-2026-1340
影響產品	Ivanti Endpoint Manager Mobile
解決辦法	根據官方網站釋出的解決方式進行修補： https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

- 內容說明：

  Ivanti Endpoint Manager Mobile (EPMM)是一款移動設備管理解決方案，能集中管理 iOS、Android、macOS 和 Windows 設備。日前發布安全性更新已修補 2 個重大資安漏洞(CVE-2026-1281 和 CVE-2026-1340，皆為 CVSS：9.8)，前述漏洞皆為程式碼注入漏洞，允許未經身分驗證的攻擊者執行遠端程式碼。

- 影響平台：
  - Ivanti Endpoint Manager Mobile 12.5.0.0 (含)更早版本
  - Ivanti Endpoint Manager Mobile 12.5.1.0 (含)更早版本
  - Ivanti Endpoint Manager Mobile 12.6.0.0 (含)更早版本
  - Ivanti Endpoint Manager Mobile 12.6.1.0 (含)更早版本
  - Ivanti Endpoint Manager Mobile 12.7.0.0 (含)更早版本
- 資料來源：
  1. Security Advisory Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281 & CVE-2026-1340)
  2. CVE-2026-1281
  3. CVE-2026-1340

2.3.2 OpenSSL函式庫存在重大資安漏洞(CVE-2025-15467)

CVE 編號	CVE-2025-15467
影響產品	OpenSSL libray
解決辦法	請更新至以下版本： OpenSSL library 3.6.1(含)之後版本 OpenSSL library 3.5.5(含)之後版本 OpenSSL library 3.4.4(含)之後版本 OpenSSL library 3.3.6(含)之後版本 OpenSSL library 3.0.19(含)之後版本

- 內容說明：

  OpenSSL 是開源的加密工具庫，主要用於安全通訊、SSL/TLS 協定實作及憑證管理，支援多種加密演算法，廣泛應用於伺服器與應用程式。近期 OpenSSL 發布安全性更新，修補重大資安漏洞(CVE-2025-15467，CVSS：9.8)，此為堆疊緩衝區溢位漏洞，可能導致程式異常終止，引發拒絕服務(DoS)攻擊，甚至可能造成遠端程式碼執行。

- 影響平台：
  - OpenSSL library 3.6.0 至 3.6.1(不含)版本
  - OpenSSL library 3.5.0 至 3.5.5(不含)版本
  - OpenSSL library 3.4.0 至 3.4.4(不含)版本
  - OpenSSL library 3.3.0 至 3.3.6(不含)版本
  - OpenSSL library 3.0.0 至 3.0.19(不含)版本
- 資料來源：
  1. OpenSSL library
  2. CVE-2025-15467

2.3.3 n8n存在重大資安漏洞(CVE-2026-1470)

CVE 編號	CVE-2026-1470
影響產品	n8n
解決辦法	請更新至以下版本： n8n 1.123.17(含)之後版本 n8n 2.4.5(含)之後版本 n8n 2.5.1(含)之後版本

- 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。近期發布重大資安漏洞公告(CVE-2026-1470，CVSS：9.9)，此為遠端程式碼執行漏洞，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，可能導致未經授權的敏感資料遭存取、工作流程被竄改，以及執行系統層級操作。

- 影響平台：
  - n8n 1.123.17(不含)之前版本
  - n8n 2.0.0 至 2.4.5(不含)之前版本
  - n8n 2.5.0 至 2.5.1(不含)之前版本
- 資料來源：
  1. n8n security
  2. CVE-2026-1470

2.3.4 Microsoft Office 存在高風險資安漏洞(CVE-2026-21509)

CVE 編號	CVE-2026-21509
影響產品	Microsoft Office
解決辦法	根據官方網站釋出的解決方式進行修補： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

- 內容說明：

  Microsoft Office 存在安全功能繞過(Security Feature Bypass)漏洞(CVE-2026-21509，CVSS：7.8)，允許未經身分驗證的攻擊者可透過發送惡意 Office 文件並誘使用戶開啟，進而繞過元件物件模型(Component Object Model, COM)與物件連結與嵌入(Object Linking andEmbedding, OLE)防護機制，使原本應該被阻擋之 COM/OLE 控制元件仍能執行。

  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：
  - Microsoft 365 Apps for Enterprise
  - Microsoft Office 2016
  - Microsoft Office 2019
  - Microsoft Office LTSC 2021
  - Microsoft Office LTSC 2024
- 資料來源：
  1. Microsoft Office 安全性功能略過缺陷
  2. CVE-2026-21509

2.3.5 Cisco Meeting Management 存在重大資安漏洞(CVE-2026-20098)

CVE 編號	CVE-2026-20098
影響產品	Cisco Meeting Management
解決辦法	請更新至以下版本： Cisco Meeting Management 3.12.1 MR (含)之後版本

- 內容說明：

  Cisco Meeting Management 提供管理員網頁介面，並監控管理視訊會議，包括新增/移除參與者、靜音、變更畫面佈局及啟動錄影等功能。近日 Cisco 發布重大資安公告(CVE-2026-20098，CVSS：8.8)，此為任意檔案上傳漏洞，可能允許經過身分驗證的遠端攻擊者，上傳任意檔案、執行任意命令，並將受影響的系統權限提升至 root。

  備註：若要利用此漏洞，攻擊者至少擁有視訊操作員的有效使用者憑證。

- 影響平台：
  - Cisco Meeting Management 3.12(含)之前版本
- 資料來源：
  1. Cisco Meeting Management Arbitrary File Upload Vulnerability
  2. CVE-2026-20098

2.3.6 n8n存在重大資安漏洞(CVE-2026-25049)

CVE 編號	CVE-2026-25049
影響產品	n8n
解決辦法	請更新至以下版本： n8n 1.123.17(含)之後版本 n8n 2.5.2(含)之後版本

- 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。近期發布重大資安漏洞公告(CVE-2026-1470，CVSS 4.x：9.4)，此漏洞允許經身分驗證且擁有建立或修改工作流程權限的攻擊者，可利用特製的工作流程參數表達式，在執行 n8n 主機上觸發未經授權的系統指令。

- 影響平台：
  - n8n 1.123.17(不含)之前版本
  - n8n 2.5.2(不含)之前版本
- 資料來源：
  1. n8n security
  2. CVE-2026-25049

2.3.7 FortiClientEMS存在重大資安漏洞(CVE-2026-21643)

CVE 編號	CVE-2026-21643
影響產品	FortiClientEMS
解決辦法	請更新至以下版本： FortiClientEMS 7.4.5 (含)之後版本

- 內容說明：

  FortiClientEMS 是 Fortinet 旗下一款端點管理伺服器，用於集中管理 FortiClient 代理程式，支持端點部署、設定與監控。近日發布重大資安漏洞公告(CVE-2026-21643，CVSS：9.8)，此為 SQL 注入漏洞，可能允許未經身分驗證的攻擊者，透過精心設計的 HTTP 請求執行未經授權的程式碼或命令。

- 影響平台：
  - FortiClientEMS 7.4.4 (含)之前版本
- 資料來源：
  1. SQLi in administrative interface
  2. CVE-2026-21643

2.3.8 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2026-23687,CVE-2026-0509,CVE-2026-0488
影響產品	SAP NetWeaver AS ABAP and ABAP Platform、CRM、S/4HANA
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/february-2026.html

- 內容說明：

  【CVE-2026-23687，CVSS：8.8】

  此漏洞存在於 SAP NetWeaver AS ABAP and ABAP Platform，允許經過身分驗證且具有普通權限的攻擊者，取得有效的簽章資訊後，將更新後的簽章 XML 文件傳送給驗證端進行驗證。

  【CVE-2026-0509，CVSS：9.6】

  此漏洞存在於 SAP NetWeaver AS ABAP and ABAP Platform，允許經過身分驗證的低權限攻擊者，於未取得 S_RFC 授權時，可執行後端遠端函式呼叫。

  【CVE-2026-0488，CVSS：9.9】

  經過身分驗證的攻擊者可利用 SAP CRM and SAP S/4HANA(腳本編輯器)中通用函數模組呼叫漏洞，執行未經授權的關鍵功能，包含執行任意 SQL 語法。

- 影響平台：

  【CVE-2026-23687】

  - SAP NetWeaver AS ABAP and ABAP Platform Version(s) - SAP_BASIS 700, SAP_BASIS 701, 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 804, SAP_BASIS 916, SAP_BASIS 917, SAP_BASIS 918

【CVE-2026-0509】

- SAP NetWeaver Application Server ABAP and ABAP Platform Version(s) - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 9.19

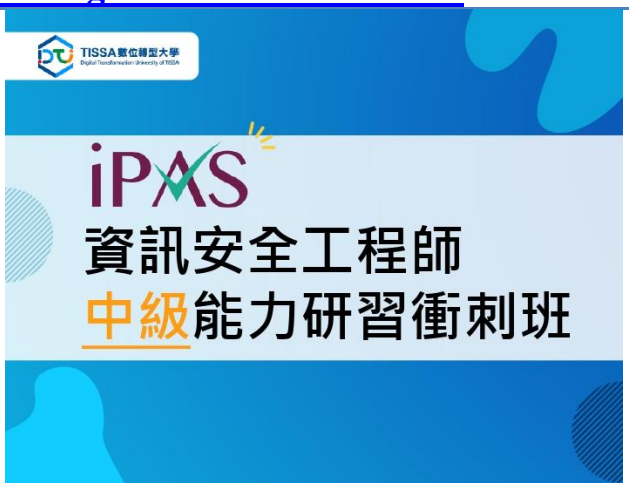
【CVE-2026-0488】

- SAP CRM and SAP S/4HANA (Scripting Editor) Version(s) - S4FND 102, 103, 104, 105, 106, 107, 108, 109, SAP_ABA 700, WEBCUIF 700, 701, 730, 731, 746, 747, 748, 800, 801

- 資料來源：
  1. SAP Security Patch Day - February 2026
  2. CVE-2026-23687
  3. CVE-2026-0509
  4. CVE-2026-0488

第 3 章、資安研討會及活動

- **資安研討會**

【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** **security@tissa.org.tw**
【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：

華苓科技｜Docpedia - SQL Injection	
TVN / CVE ID	TVN-202602001 / CVE-2026-2094
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	Docpedia 3.0
問題描述	Docpedia存在SQL Injection漏洞，已通過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	請安裝修補程式 DP4 HotFix_057
公開日期	2026-02-06
相關連結	https://www.twcert.org.tw/tw/cp-132-10697-6a30b-1.html
華苓科技｜AgentFlow - 存在3個漏洞	
TVN / CVE ID	TVN-202602002 / CVE-2026-2095, CVE-2026-2096, CVE-2026-2097
CVSS	CVE-2026-2095： 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVE-2026-2096： 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVE-2026-2097： 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	Agentflow 所有版本
問題描述	CVE-2026-2095(Authentication Bypass)：

	未經身分鑑別之遠端攻擊者可利用特定功能取得任意使用者驗證憑證，進而以任意使用者身分登入系統。 CVE-2026-2096(Missing Authenticaton)： 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-2026-2097(Arbitrary File Upload)： 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	CVE-2026-2095, CVE-2026-2096： 請參考以下官方說明採取緩解措施 https://forum.flowring.com/post/view?bid=72&id=45611&tpg=1&ppg=1&sty=1#45939 CVE-2026-2097： 聯繫廠商確認應對措施
公開日期	2026-02-06
相關連結	**https://www.twcert.org.tw/tw/cp-132-10699-49c0b-1.html**
桓基科技｜C&Cm@il - Missing Authentication	
TVN / CVE ID	TVN-202602004 / CVE-2026-2234
CVSS	9.1 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
影響產品	C&Cm@il套件olln-base 7.0-978(不含)以前版本
問題描述	CVE-2026-2234(Missing Authentication)： 未經身分鑑別之遠端攻擊者可讀取與修改任意使用者信件內容。
解決方法	更新套件olln-base 7.0-978(含)以後版本

公開日期	2026-02-09
相關連結	https://www.twcert.org.tw/tw/cp-132-10703-3d02f-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2月28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/**