TWCERT/CC 資安情資電子報

2026 年 5 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

歐盟 CRA 進入強制合規階段！全球聯網製造商迎戰 SBOM 管理挑戰

《網路韌性法案》（Cyber Resilience Act, CRA）執行時程已正式進入倒數階段，最具衝擊力的第 14 條「漏洞通報義務」將於2026年9月11日 正式強制執行。屆時，所有進入歐盟市場的具備數位功能產品，若得知存在「活躍漏洞利用（Actively Exploited Vulnerability）」，製造商必須在24小時內發布早期預警。這項嚴格的法規不僅是歐盟境內的法律義務，更對全球電子製造供應鏈帶來巨大的連鎖反應，迫使廠商必須全面升級產品開發與漏洞應變機制。

根據法案最終公告條款，製造商在獲悉漏洞後將面臨極具挑戰性的時間壓力，企業必須在發現漏洞的24小時內，透過歐盟「單一通報平台(SRP)」向當地電腦安全事件應變團隊 (CSIRT) 及歐盟網路安全局(ENISA) 發出早期預警，並於72 小時內補齊詳細的漏洞災損評估。此外，在具備可用的矯正或緩解措施後 14 天內，製造商還需提交最終報告，若屬於重大資安事件則放寬至一個月內提交。一旦未能履行這項通報義務或產品不符資安規範，違規廠商最高將面臨1,500萬歐元或全球年營收2.5%的高額罰鍰，相關產品也可能遭受下架、召回或限制銷售等嚴厲處分。

這項涵蓋所有已在市場流通數位產品的生命週期追溯機制，正促使軟體材料清單（SBOM）成為實務上不可或缺的隱性先決條件。由於法規限定的通報時效極短，製造商若缺乏清晰的產品組件清單，將難以在24 小時內精準判定哪些既有產品或韌體版本正受到該特定漏洞的威脅。因此，建立標準化、動態化的 SBOM 管理架構，已不再只是單純的技術選項，而是全球設備大廠全面推進市場主動合規的關鍵核心。

在技術落實層面上，這場變革正引領全球科技業從「被動防禦」走向「內建安全」的深層轉型。廠商除了必須導入CycloneDX 或 SPDX 等國際標準格式的 SBOM 管理工具，並結合自動化漏洞掃描器執行全天監控外，也必須嚴格遵循法規中對預設安全配置的強制要求。這意味著設備開發者在產品出廠前，就應落實 Security by Design 原則，包含關閉不必要通訊埠、取消任何預設弱密碼等防禦方法，避免產品上市後成為攻擊者可利用的弱點。

面對即將到來的法規浪潮，製造商與供應鏈企業應立即採取以下前瞻性的韌性強化措施：

1. 立即清查產品線並導入SBOM：首要任務是立即清查所有外銷歐盟的產品清單，並優先針對核心產品產製完整的 SBOM，確保能隨時掌握第三方套件與開源軟體元件狀況。
2. 建立漏洞應處機制與內部演練：針對法規要求的「24小時與72小時」極短時限，企業須明確制定內部應變與通報流程，透過跨部門的實戰演練，確保產品、資安與法務團隊能在時限內完成通報判定。
3. 成立 PSIRT團隊並接軌國際聯防：建議企業內部應積極建置「產品資安事件應變團隊 (PSIRT)」，並與國際漏洞資料庫進行即時對接，建立標準化的應變能量。
4. 推動深層技術升級與法規追蹤：企業技術升級並以Security by Design 為原則，在產品設計開發初期即考量其安全性，同時密切關注歐盟委員會對於「符合性評估」的具體細則演進，以隨時動態調整合規策略。

- 相關連結
  1. Cyber Resilience Act - Reporting obligations
  2. EU Cyber Resilience Act: Key 2026 milestones toward CRA compliance
  3. One Year Countdown to EU CRA Compliance - September 11, 2026, Changes Everything
  4. 你的漏洞不再只是你的漏洞：CRA推動漏洞通報機制

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 「裝置碼」釣魚攻擊成新興威脅，企業與組織成主要目標

近期微軟資安研究團隊與資安廠商觀察指出，攻擊者正大量利用名為「EvilTokens」的新興網路釣魚服務平台（PhaaS），結合人工智慧與自動化工具，針對企業與組織發動「裝置碼(Device Code)」釣魚攻擊。駭客透過社交工程手段，誘騙使用者於官方合法頁面完成授權程序，藉此成功繞過多因子驗證(MFA)並接管帳號，進而竊取內部敏感資料。資安專家特別指出，由於微軟Azure與Google兩大雲端平台在OAuth 2.0裝置碼機制的權限實作上存在差異，微軟環境面臨更為嚴重威脅。

國家資通安全研究院日前亦發布資安提醒指出，攻擊者正濫用「裝置碼」登入機制發動釣魚攻擊。「裝置碼」登入機制原本是為了智慧電視、物聯網（IoT）等不便輸入帳號密碼的設備所設計的驗證流程。然而，此項便利功能現已成為駭客濫用的目標。

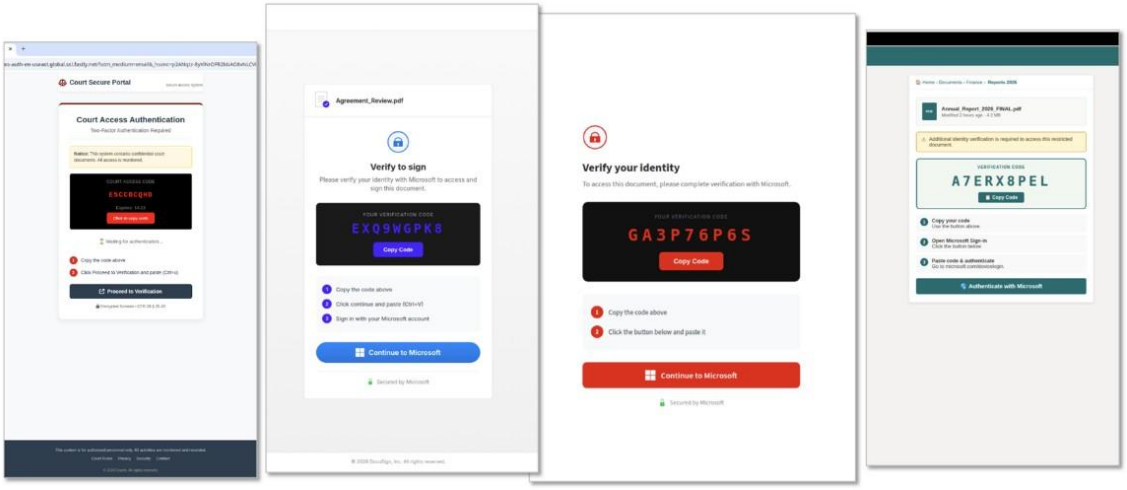

圖1：裝置程式碼釣魚登入頁面範例。資料來源：proofpoint

攻擊者通常會發送客製化的社交工程郵件，如假冒企業內部設備管理人員，聲稱會議室的智慧電視連線失效，要求受害者協助掃描或輸入驗證碼進行驗證。當受害者被引導至真實的微軟官方裝置登入頁面，並輸入由駭客端動態生成的裝置碼並完成多因子驗證後，實際上等同於替攻擊者的登入請求完成認證，由於整個驗證流程與輸入網址皆為微軟官方真實服務。在傳統資安宣導中「檢查網址是否偽造」的防範方式對此攻擊完全無效，導致受害者極易降低戒心而受害。

一旦攻擊成功，攻擊者便能順利獲取登入權限並全面接管帳號，進而存取該帳號權限內的OneDrive雲端檔案、Outlook信件等敏感資料。此類攻擊可能進一步引發商業電子郵件詐騙與企業內部網路的橫向移動，進而成為攻擊者佈署勒索軟體的潛伏據點。

圖2：裝置碼（Device Code）社交工程攻擊示意流程。資料來源：資安院

資安廠商 Huntress 進一步分析兩大主要雲端平台在 OAuth 2.0 裝置碼機制上的實作差異，發現二者在遭受此類攻擊時的損害程度有顯著不同。在微軟 Azure 環境中，由於機制允許攻擊者在請求中指定資源與客戶端 ID(Client ID)，駭客可藉由裝置碼釣魚取得極高權限的存取權杖(Access Token)。這使得駭客能利用 Microsoft Graph API 讀取電子郵件、存取敏感檔案，甚至惡意註冊裝置以竊取主要重新整理權杖(Primary Refresh Token, PRT)，達成全面的帳號劫持；在Google 環境中，Google 對於裝置碼流程的權限限制極為嚴格，僅允許極少數特定範圍的授權。這項設計大幅削弱攻擊者利用該機制進行後續橫向移動的能力，因此在 Google 環境中造成的危害較低於微軟環境。

資安院提醒，此類攻擊是透過微軟合法官方頁面完成登入與MFA驗證，使用者易降低戒心而進行操作，建議企業與組織應儘速檢視內部雲端環境，並採取以下防護措施：

1. 嚴格限制或封鎖裝置碼流程：企業應評估組織內部設備管理之

實際需求，若無必要，建議透過「條件式存取原則(Conditional Access Policy)」全面封鎖裝置碼流程；若無法全面封鎖，則應採用嚴格的白名單機制，僅允許獲得批准的使用者、信任之作業系統或特定IP網段使用此功能。

2. 強化登入日誌監控與異常授權撤銷：資安團隊應加強監控登入日誌中驗證協定為Device Code 的活動。若發現異常的登入請求，或使用者在非預期時間點進行裝置碼驗證，應即時撤銷相關帳號的登入授權與所有連線階段。

3. 提升員工針對新型態攻擊的資安意識：傳統的釣魚防範訓練已不足以應對此類新型態威脅。組織應教育員工，面對任何「請求輸入設備碼」、「授權應用程式」或「進行額外身分驗證」的郵件與訊息時應提高警覺，切勿在未確認的情況下輸入來自外部或未受信任來源的裝置碼。

- 相關連結

1. Inside an AI-enabled device code phishing campaign
2. Device Code Phishing is an Evolution in Identity Takeover
3. How EvilTokens Turbocharges Old School Phishing with AI
4. How OAuth 2.0 Device Code Phishing Works in Azure and Google
5. 駭客結合AI與自動化工具濫用裝置代碼機制，資安院提醒授權帳號可能遭盜用或敏感資料外洩

2.2 軟硬體系統資安議題

2.2.1 駭客組織 UAT-8616 鎖定 Cisco Catalyst SD-WAN 滿分漏洞發動攻擊

Cisco近日發布重大安全性公告，揭露並修復旗下Catalyst SD-WAN網路架構中一項高嚴重性的身分驗證繞過漏洞(CVE-2026-20182，CVSS：10.0)。該漏洞將允許未經身分驗證的遠端攻擊者，透過發送特製請求直接繞過身分驗證機制，進而取得內部高權限帳號管理帳號(non-root)。攻擊者一旦掌握此權限，便可透過存取「NETCONF」服務，藉此任意竄改SD-WAN 的網路配置、建立惡意網路節點並深入攻擊企業與組織內部網路。目前美國網路安全與基礎設施安全局(CISA)已將此漏洞納入已知漏洞目錄(KEV)；同時亦有情資顯示，駭客組織 UAT-8616 正積極利用此漏洞發動攻擊，呼籲相關用戶務必提高警覺，並儘速採取對應的防禦與修補措施。

本次受影響的產品範圍相當廣泛，無論企業是採用本地端建置(On-Prem Deployment)或由Cisco代管的雲端版本(如Cisco SD-WAN Cloud)皆受到此漏洞影響。具體受影響的系統包含原名為SD-WAN vSmart的Cisco Catalyst SD-WAN Controller，以及原名為SD-WAN vManage的Cisco Catalyst SD-WAN Manager。

資安公司Rapid7調查指出，該核心問題在於處理 DTLS 協定的vdaemon 服務中，該漏洞源自於系統的對等身分驗證機制存在缺陷有關。當外部攻擊者發起連線並在特定的回應訊息(CHALLENGE_ACK)，將自身的設備類型宣告為特定節點時，系統的驗證程式可能會在未完成憑證檢查的情況下直接放行，導致攻擊者得以偽裝成受信任的內部對等節點。

Rapid7進一步指出，成功繞過安全驗證之後，攻擊者能夠把未授權的SSH公鑰寫入系統內部高權限帳號(vmanage-admin)中，攻擊者便能順理成章地以該高權限帳號身分，透過TCP通訊埠 830 存取 NETCONF 服務，由於NETCONF服務可用於管理網路設備組態，若漏洞遭成功利用，攻擊者可能進一步竄改SD-WAN 網路組態，對企業網路管理與營運穩定性造成影響。

```
msf auxiliary(admin/networking/cisco_sdwan_vhub_auth_bypass) > run
[*] Running module against 192.168.80.11
[*] Phase 1: DTLS handshake with self-signed certificate
[*] DTLS handshake succeeded (self-signed cert accepted)
[*] Phase 2: Waiting for CHALLENGE from server
[*] CHALLENGE received (580 bytes)
[*] Phase 3: Sending CHALLENGE_ACK as vHub (authentication bypass)
[*] Phase 4: Waiting for server response to CHALLENGE_ACK
[*] No immediate response (server is waiting for Hello)
[*] Phase 5: Sending Hello as authenticated peer
[+] Hello response received - authenticated as vHub peer
[*] Phase 6: Injecting SSH public key into vmanage-admin authorized_keys
[*] Generating RSA 2048-bit SSH keypair
[*] SSH private key saved to loot: /home/cryptocat/.msf4/loot/20260501113926_default_192.168.80.11_
cisco.sdwan.sshk_256631.pem
[+] Connect to the NETCONF service via:
ssh -i /home/cryptocat/.msf4/loot/20260501113926_default_192.168.80.11_cisco.sdwan.sshk_256631.pem
vmanage-admin@192.168.80.11 -p 830
[*] Server responded with REGISTER_TO_VMANAGE (SSH key accepted)
[+] Authentication bypass and SSH key injection completed!
[*] Auxiliary module execution completed
```

圖1：利用vHub驗證繞過和SSH金鑰注入示意圖。資料來源：Rapid7

思科威脅情報團隊 Talos 表示，駭客組織UAT-8616目前正積極利用此零時差漏洞發動攻擊，其攻擊手法包含：利用漏洞入侵、新增惡意SSH金鑰、竄改 NETCONF 組態，並進一步將權限提升至root 層級，進而控制企業與組織的內部網路。

為確保企業與組織的網路安全，建議管理團隊立即採取以下應變措施：

1. 立即實施系統更新：儘速將系統升級至 Cisco 官方釋出的最新修補版本，以徹底修補此安全漏洞。
2. 檢查身分驗證日誌：建議管理員審查系統日誌，確認是否有來自未知或未經授IP的連線紀錄，特別需針對vmanage-admin帳號的公鑰登入 (Accepted publickey) 進行異常稽核。
3. 監控異常對等連線：檢查日誌是否有可疑的對等連線事件 (Peering Events)，例如在非預期時間點、來源IP無法辨識，或是設備類型與現有網路架構不符的連線行為。

- 相關連結

1. Ongoing exploitation of Cisco Catalyst SD-WAN vulnerabilities
2. CVE-2026-20182: Critical authentication bypass in Cisco Catalyst SD-WAN Controller (FIXED)
3. Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability

2.3 軟硬體漏洞資訊

2.3.1 Palo Alto Networks PAN-OS存在重大資安漏洞(CVE-2026-0300)

CVE 編號	CVE-2026-0300
影響產品	Palo Alto Networks PAN-OS
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-2026-0300

- 內容說明：

  Palo Alto Networks 的防火牆作業系統 PAN-OS 的 User-ID 驗證入口網站服務存在緩衝區溢位漏洞(CVE-2026-0300，CVSS ：9.3)，此漏洞允許未經身分驗證的攻擊者透過發送特製的資料，在 PA 系列和 VM 系統防火牆上，以 root 權限執行任意程式碼。

- 影響平台：
  - PAN-OS 12.1.4-h5(不含)以前版本
  - 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-h13(不含)以前版本
  - PAN-OS 11.2.10-h6(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

- 資料來源：
  1. CVE-2026-0300

2.3.2 Apache ActiveMQ存在高風險安全漏洞(CVE-2026-40466與CVE-2026-41044)，請儘速確認並進行修補

CVE 編號	CVE-2026-40466,CVE-2026-41044
影響產品	Apache ActiveMQ
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://activemq.apache.org/security-advisories.data/CVE-2026-40466-announcement.txt https://activemq.apache.org/security-advisories.data/CVE-2026-41044-announcement.txt

- 內容說明：

  研究人員發現 Apache ActiveMQ 存在 2 個高風險安全漏洞(CVE-2026-40466 與 CVE-2026-41044)，類型包含不當輸入驗證(Improper Input Validation)與程式碼注入(Code Injection)，已通過身分鑑別之遠端攻擊者可利用此漏洞，使 ActiveMQ 載入惡意設定檔，進而執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - Apache ActiveMQ Broker 5.19.6(不含)以前版本
  - Apache ActiveMQ Broker 6.0.0 至 6.2.5(不含)版本
  - Apache ActiveMQ All 5.19.6(不含)以前版本
  - Apache ActiveMQ All 6.0.0 至 6.2.5(不含)版本
  - Apache ActiveMQ 5.19.6(不含)以前版本
  - Apache ActiveMQ 6.0.0 至 6.2.5(不含)版本
- 資料來源：
  1. CVE-2026-40466
  2. CVE-2026-41044
  3. CVE-2026-40466-announcement.txt
  4. CVE-2026-41044-announcement.txt

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

CVE 編號	CVE-2026-5786,CVE-2026-5787
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://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?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，近日 Ivanti 發布重大資安漏洞公告。

  【CVE-2026-5786，CVSS：8.8】

  此為存取控制不當漏洞，允許經身分驗證的遠端攻擊者獲取管理存取權限。

  【CVE-2026-5787，CVSS：8.9】

  此為憑證驗證不當，允許未經身分驗證的遠端攻擊者可冒充已註冊的 Sentry 主機並取得有效的 CA 簽章用戶端憑證。

- 影響平台：
  - Ivanti Endpoint Manager Mobile 12.8.0.0(含)及更早版本
- 資料來源：
  1. May 2026 Security Advisory Ivanti Endpoint Manager Mobile (EPMM) (Multiple CVEs)
  2. CVE-2026-5786
  3. CVE-2026-5787

2.3.4 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2026-34260,CVE-2026-34263
影響產品	SAP S/4HANA、Commerce cloud
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/may-2026.html

- 內容說明：

  【CVE-2026-34260，CVSS：9.6】

  SAP S/4HANA (SAP Enterprise Search for ABAP) 存在 SQL 注入漏洞，允許經過身分驗證的攻擊者，透過 user-controlled 注入惡意 SQL 語法，並在未經適當驗證或過濾的情況下傳至底層資料庫，導致攻擊者可能取得未經授權的敏感資料庫存取權限，影響應用程式的機密性與可用性。

  【CVE-2026-34263，CVSS：9.6】

  SAP Commerce cloud 允許未經驗證的攻擊者執行惡意組態上傳與程式碼注入，導致任意伺服器端程式碼執行，可能影響應用程式的機密性、完整性與可用性。

- 影響平台：

  【CVE-2026-34260】

  - SAP S/4HANA (SAP Enterprise Search for ABAP)
    Version(s) - 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

  【CVE-2026-34263】

  - SAP Commerce cloud
    Version(s) - HY_COM 2205, COM_CLOUD 2211, 2211-JDK21

- 資料來源：
  1. SAP Security Patch Day - May 2026
  2. CVE-2026-34260
  3. CVE-2026-34263

2.3.5 Ivanti旗下Endpoint Manager存在高風險資安漏洞(CVE-2026-8111)

CVE 編號	CVE-2026-8111
影響產品	Ivanti Endpoint Manager
解決辦法	請更新至 Ivanti Endpoint Manager 2024 SU6 (含)之後版本

- 內容說明：

  Ivanti 旗下的 Endpoint Manager(EPM)是一款專門針對裝置管理的系統，提供管理和保護 Windows、macOS 和 Linux 裝置。近期 Ivanti 發布重大資安漏洞公告(CVE-2026-8111，CVSS：8.8)，此為 SQL 注入漏洞，允許經身分驗證的遠端攻擊者實現遠端程式碼執行。

- 影響平台：
  - Ivanti Endpoint Manager 2024 SU6(不含)以前版本
- 資料來源：
  1. Security Advisory Ivanti Endpoint Manager (EPM) May 2026
  2. CVE-2026-8111

2.3.6 Ivanti旗下Xtraction存在高風險資安漏洞(CVE-2026-8043)

CVE 編號	CVE-2026-8043
影響產品	Ivanti Xtraction
解決辦法	請更新至 Ivanti Xtraction 2026.2(含)之後版本

- 內容說明：

  Ivanti 旗下的 Xtraction 是一套 IT 報表與資料視覺化平台，可將不同 IT 系統的資料整合至同一儀表板，方便即時查看與分析。近期 Ivanti 發布重大資安漏洞公告(CVE-2026-8043，CVSS：9.6)，此漏洞允許經身分驗證的攻擊者讀取敏感檔案，並將任意 HTML 檔案寫入網站目錄。

- 影響平台：
  - Ivanti Xtraction 2026.1(含)以前版本
- 資料來源：
  1. Security Advisory - Ivanti Xtraction (CVE-2026-8043)
  2. CVE-2026-8043

2.3.7 Fortinet旗下FortiAuthenticator 存在重大資安漏洞(CVE-2026-44277)

CVE 編號	CVE-2026-44277
影響產品	Fortinet FortiAuthenticator
解決辦法	請更新至以下版本： FortiAuthenticator 8.0.3(含)之後版本、 FortiAuthenticator 6.6.9(含)之後版本、 FortiAuthenticator 6.5.7(含)之後版本

- 內容說明：

  Fortinet 旗下 FortiAuthenticator 產品存在不當存取控制漏洞(CVE-2026-44277，CVSS：9.8)，未經身分驗證的攻擊者可能透過特製的請求，執行未經授權的程式碼或命令。

- 影響平台：
  - FortiAuthenticator 8.0.0 版本、
  - FortiAuthenticator 8.0.2 版本、
  - FortiAuthenticator 6.6.0 至 6.6.8 版本、
  - FortiAuthenticator 6.5.0 至 6.5.6 版本
- 資料來源：
  1. Improper access control on API endpoints
  2. CVE-2026-44277

2.3.8 Fortinet旗下FortiSandbox、FortiSandbox Cloud 和 FortiSandbox PaaS存在重大資安漏洞(CVE-2026-26083)

CVE 編號	CVE-2026-26083
影響產品	Fortinet FortiSandbox、FortiSandbox Cloud、FortiSandbox PaaS
解決辦法	請更新至以下版本： FortiSandbox 5.0.2(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 5.0.2(含)之後版本、 FortiSandbox PaaS 4.4.9(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-2026-26083，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 5.0.1 版本
  - FortiSandbox 4.4.0 至 4.4.8 版本
  - FortiSandbox Cloud 24 所有版本
  - FortiSandbox Cloud 23 所有版本
  - FortiSandbox Cloud 5.0.2 至 5.0.5 版本
  - FortiSandbox PaaS 23.4 所有版本
  - FortiSandbox PaaS 23.3 所有版本
  - FortiSandbox PaaS 23.1 所有版本
  - FortiSandbox PaaS 22.2 所有版本
  - FortiSandbox PaaS 22.1 所有版本

- FortiSandbox PaaS 21.4 所有版本
- FortiSandbox PaaS 21.3 所有版本
- FortiSandbox PaaS 5.0.0 至 5.0.1 版本
- FortiSandbox PaaS 4.4.5 至 4.4.8 版本

- 資料來源：
  1. Incorrect global authorization
  2. CVE-2026-26083

2.3.9 Cisco Catalyst SD-WAN 存在重大資安漏洞(CVE-2026-20182)

CVE 編號	CVE-2026-20182
影響產品	Cisco Catalyst SD-WAN
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-sdwan-rpa2-v69WY2SW

- 內容說明：

  Cisco Catalyst SD-WAN 是 Cisco 以雲端為中心的軟體定義廣域網路架構，提供集中管理、安全加密及應用效能優化，確保多雲環境的可靠連線，近日 Cisco 發布重大資安公告。

  【CVE-2026-20182，CVSS：10.0】

  此漏洞存在於 Cisco Catalyst SD-WAN Controller (formerly vSmart) 與 Catalyst SD-WAN Manager (formerly vManage)，允許遠端攻擊者發送特製請求繞過身分驗證，取得內部高權限帳號 (non-root)。攻擊者後續可利用高權限帳號存取 NETCONF，修改 SD-WAN 網路架構配置，建立惡意網路節點並深入攻擊企業/組織網路。

  註：Cisco Catalyst SD-WAN Controller (formerly vSmart) 與 Cisco Catalyst SD-WAN Manager (formerly vManage) 已被發現積極利用於攻擊活動，請儘速採取應變措施。

- 影響平台：
  - Cisco Catalyst SD-WAN On-Prem Deployment
  - Cisco SD-WAN Cloud-Pro
  - Cisco SD-WAN Cloud (Cisco Managed)
  - Cisco SD-WAN for Government (FedRAMP)

- 資料來源：
  1. Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability
  2. CVE-2026-20182

2.3.10 Cisco Secure Workload 存在重大資安漏洞(CVE-2026-20223)

CVE 編號	CVE-2026-20223
影響產品	Cisco Secure Workload
解決辦法	請更新至以下版本： Cisco Secure Workload 3.10.8.3(含)之後版本 Cisco Secure Workload 4.0.3.17(含)之後版本

- 內容說明：

  Cisco Secure Workload 存在未經授權的 API 存取漏洞(CVE-2026-20223，CVSS：10.0)，可能允許未經身分驗證的遠端攻擊者，以 Site Admin 的權限存取網站資源。

- 影響平台：
  - Cisco Secure Workload 3.9(含)以前版本
  - Cisco Secure Workload 3.10.8.3(不含)以前版本
  - Cisco Secure Workload 4.0.3.17(不含)以前版本
- 資料來源：
  1. Cisco Secure Workload Unauthorized API Access Vulnerability
  2. CVE-2026-20223

2.3.11 Microsoft 旗下SharePoint Server 存在重大資安漏洞(CVE-2026-45659)

CVE 編號	CVE-2026-45659
影響產品	Microsoft SharePoint Server
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-2026-45659

- 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-2026-45659，CVSS：8.8)，此漏洞為不受信任資料反序列化漏洞，允許經身分驗證的攻擊者可透過網路執行程式碼。

- 影響平台：
  - Microsoft SharePoint Enterprise Server 2016 16.0.5552.1002(不含)之前版本
  - Microsoft SharePoint Server 2019 16.0.10417.20128(不含)之前版本
  - Microsoft SharePoint Server Subion Edition 16.0.19725.20280(不含)之前版本
- 資料來源：
  1. Microsoft SharePoint 遠端執行程式碼弱點
  2. CVE-2026-45659

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**
【資安院】資安長高階領導班第4期	
活動時間	**115年6月26日至7月24日，每星期五9:00至16:30，合計30小時**
活動地點	**JR 東日本大飯店台北(台北市中山區南京東路三段 133 號)**
活動網站	**https://forms.gle/u87UwQqP2fH3a22B9**
活動概要	 **【費用】** 付費 報名截止： 115年6月15日 23:59 **【活動內容 / Event Deails】** 隨著數位科技成為現代社會不可或缺的一部分，資訊安全已不侷限於技術部門的管理與防護。資安主管在企業中扮演著關鍵角色，必須具備高階決策思維，將資安防護與企業整體營運戰略緊密結合。

	為提升各產業的數位韌性，國家資通安全研究院持續主辦【資安長|高階領導班】培訓計畫，專為企業高階主管設計，匯集業界資深資安專家授課，針對資安長職涯發展量身打造。 **【主辦單位】國家資通安全研究院** **【協辦單位】中華民國資訊軟體服務商業同業協會、資安長聯誼會、台灣資安主管聯盟** **【聯絡窗口】02-6631-3535 施小姐** **nics.tect@nics.nat.gov.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：

旭聯科技｜CTMS培訓大師 - SQL Injection	
TVN / CVE ID	TVN-202604012 / CVE-2026-7489
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	CTMS培訓大師 所有版本
問題描述	【CVE-2026-7489(SQL Injection)】 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	廠商應已提供修補程式。若尚未取得，請主動聯繫廠商。
公開日期	2026-04-30
相關連結	**https://www.twcert.org.tw/tw/cp-132-10894-1ac1f-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5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/**