TWCERT/CC 資安情資電子報

2025 年 12 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

TWCERT/CC 2025台灣資安通報應變年會：打造安全產品 串聯信任防線

台灣電腦網路危機處理暨協調中心（TWCERT/CC）於昨（3）日辦理「2025台灣資安通報應變年會」。本年度以「打造安全產品 串聯信任防線」為主題，邀集來自華碩、奧義、資策會、台達電、合勤投控、群暉科技、台灣松下等產官學界資安專家齊聚一堂，聚焦AI驅動下的資安威脅、國內通報協調機制的成果與挑戰，以及產品資安治理與PSIRT弱點通報的實務經驗，共同探討如何強化跨域協作與企業資安韌性。

數位發展部林宜敬部長於致詞中表示，面對AI、IoT與智慧製造快速普及，產品一旦上線，承載的不只是功能與效能，更包含使用者資料與品牌信任。產品資安不再只是技術議題，而是企業競爭力的重要基礎。

他指出，安全設計與安全開發流程是企業必要的基本功，愈來愈多國際法規將產品資安視為供應鏈治理的一部分，代表「安全」已成全球市場的共同語言。部長同時肯定TWCERT/CC在全年無休的事件通報、情資分享、漏洞揭露、PSIRT推動與國際組織參與上的努力，並強調資安防線需要政府、企業與使用者共同維護。

資通安全署蔡福隆署長亦表示，2025年全球資安情勢仍持續嚴峻，APT、勒索攻擊與生成式AI帶來的新威脅，使單一組織已難以獨自有效因應。本次年會以「打造安全產品、串聯信任防線」為主題，正呼應全球資安治理從「防護」走向「信任」的趨勢。他強調，在產品、服務、乃至整個供應鏈中，唯有將「安全」作為設計與管理的核心，才能贏得市場與社會的信任。署長也期盼透過本次年會的議題分享與交流，協助在場企業獲得更多前瞻洞察與實務啟發。

本次年會特別邀請多位資安專家發表專題演講，包括華碩金慶柏資安長、資安院通報應變中心孫偉哲主任、奧義智慧科技邱銘彰創辦人、資安院李婉萍經理、資策會資安所李彥震主任、資安院游家雯總監等講者，從資安趨勢、TWCERT/CC年度成果、AI攻防、Secure-by-Design設計理念、PSIRT通報治理等面向進行深入分享。

會議最後由資安院龔副院長主持高峰座談，邀請合勤投控、台達電、群暉科技與台灣松下網路安全實驗室代表，共同探討「產品資安即品牌信任」的核心價值，從設計、製造到弱點通報的完整生命週期出發，分享企業如何以行動落實產品資安治理，並呼籲產業共同打造更安全可信的資安生態。

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 OWASP 2025年Web應用安全十大威脅揭曉，存取控制漏洞位居榜首

2025年OWASP Top 10 Web應用程式安全風險清單正式公布，今年的排名出現顯著異動，反映當前資安威脅的快速演變。存取控制漏洞（Broken Access Control）持續位居榜首，而安全配置錯誤（Security Misconfiguration）與軟體供應鏈缺失（Software Supply Chain Failures）則躍升至第二、第三位，顯示企業在雲端架構與第三方組件管理上面臨更大的挑戰。

今年2025年OWASP Top 10 Web應用程式安全風險清單新增兩大類別，分別為「軟體供應鏈缺失」和「特殊情況處理不當」，同時將伺服

器端請求偽造(SSRF)合併至「存取控制漏洞」。其中，「軟體供應鏈缺失」首次進入前三，突顯開源套件與第三方服務的風險日益增加。而「加密機制失效」與「注入攻擊」雖仍列榜上，但排名下降，顯示組織針對這些漏洞已累積一定程度的防護能量。最後，新類別「特殊情況處理不當」涵蓋軟體在不可預測壓力下的表現，從錯誤處理不佳到邏輯崩潰，隨著系統互連且AI驅動的趨勢，此領域的風險正逐漸上升。詳細排名參閱圖1，各類別之說明請參閱表1。

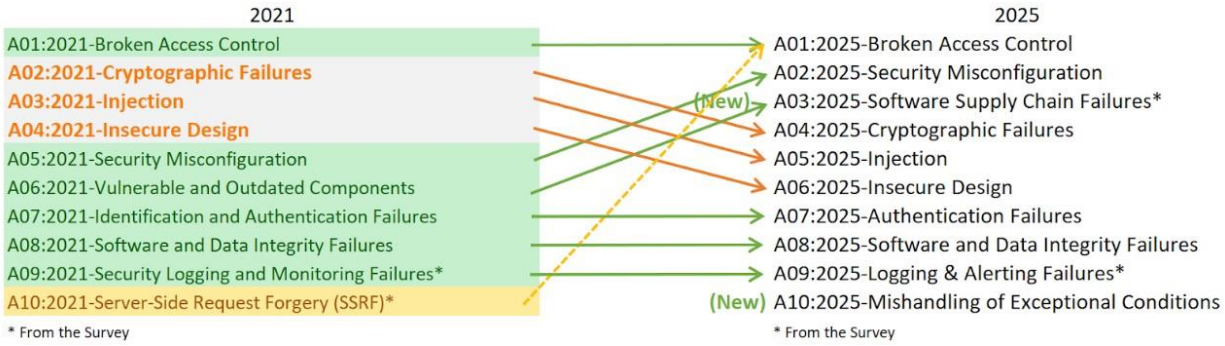


圖1：2025年OWASP Top10從2021年到2025年的變化。資料來源：OWASP Top10

OWASP 排名	類別	簡要概述
A01:2025	存取控制漏洞（Broken Access Control）	允許攻擊者繞過授權或未經授權存取
A02:2025	安全配置錯誤（Security Misconfiguration）	系統、應用程式或雲端服務設定不正確
A03:2025	軟體供應鏈缺失（Software Supply Chain Failures）	第三方軟體建置、分配或更新過程中出現中斷或其他問題
A04:2025	加密機制失效（Cryptographic Failures）	缺乏加密、加密強度不足、加密金鑰外洩等相關錯誤
A05:2025	注入攻擊（Injection）	攻擊者向輸入欄位插入惡意程式碼或命令

A06:2025	不安全設計（Insecure Design）	設計和架構缺陷等相關風險，涵蓋應用程式邏輯錯誤
A07:2025	身份驗證失敗（Authentication Failures）	攻擊者誘騙系統將無效或錯誤的使用者識別為合法使用者
A08:2025	軟體及資料完整性失效（Software or Data Integrity Failures）	未能有效防止將無效或不受信任的程式碼或資料視為可信任的有效資料
A09:2025	日誌記錄與告警（Logging & Alerting Failures）	缺乏日誌記錄與告警，導致無法偵測攻擊與漏洞，且難以快速有效進行回應
A10:2025	特殊情況處理不當（Mishandling of Exceptional Conditions）	包含開啟失敗、錯誤處理不當、邏輯錯誤以及系統可能遇到的其他異常情況

表1：2025年OWASP Top10之敘述說明。資料來源：TWCERT/CC彙整

2025年OWASP Top10的異動提醒組織，在面對這些新舊資安威脅時，資安防護必須與時俱進，針對排名變動的風險加強對策，才能有效降低資安事件發生的機率，以下是TWCERT/CC提供的建議：

1. 強化存取控制機制，採用最小權限為原則，並定期審查權限設定，避免未授權存取。
2. 完整盤點第三方元件與供應商，建立追蹤機制(如SBOM)，落實供應鏈安全評估與持續監控。
3. 建議針對對外服務網站定期執行如弱點掃描、滲透測試等安全檢測，降低潛在暴露在外之弱點遭利用之風險。
4. 增加安全身份驗證機制，要求多因子驗證(MFA)，並限制失敗登入嘗試次數。

5. 建議企業成立產品應變團隊(PSIRT)，以建置異常處理與事件回應機制，確保系統面對異常狀況時仍能維持安全。
6. 定期更新安全意識與技術訓練，掌握最新威脅與防禦技術。

- 相關連結
  1. OWASP Top 10:2025 RC1
  2. OWASP Top 10 2025: Official List, Changes, and What Developers Need to Know
  3. The 2025 OWASP Top 10: What's New and Rising in AppSec Today
  4. Two New Web Application Risk Categories Added to OWASP Top 10

2.2 新興應用資安

2.2.1 提高社交工程警覺！偽冒主管要求建群組與提供個資

TWCERT/CC近期接獲多筆外部情資分享，發現攻擊者偽冒企業內部主管名義，發起社交工程攻擊，誘使收件者開啟郵件並依照指示內容執行作業。建議通知各單位加強防範並提高警覺，若郵件內容含有可疑附件與連結，請勿點擊以免受駭。

此次情資顯示，攻擊郵件具有明顯特徵，內容多以「主管指示」、「行政需求」、「緊急任務」做為切入點，信件內容示例如下：

1. 「為便於公司管理，麻煩你建立一個專屬的公司內部 LINE 群組。建成後，請將群組的QR Code轉寄到此信箱，我稍等進群安排工作。」

2. 「請同仁提供員工清單個資資訊」

圖1：駭客偽冒公司主管要求員工提供個資之社交郵件。資料來源：TWCERT/CC整理

TWCERT/CC呼籲各組織提高警覺，並加強內部資安宣導。若收到來路不明或要求提供敏感資訊的郵件，應採取下列防範措施：

1. 提高對可疑電子郵件的警覺，務必確認郵件來源之正確性，避免點擊可疑附件或連結，以防遭受惡意程式植入或導向釣魚網站。若不慎進入疑似惡意網站，切勿輸入任何個資、帳號密碼及金融資訊。
2. 請留意寄件者資訊是否異常，並再次向主管或資訊部門確認郵件真實性。若懷疑為社交工程攻擊，應立即向資訊部門回報，以便進行後續處理。
3. 建議定期更換符合複雜性原則之密碼，並啟用多因子認證(MFA)，以提高安全防護強度，降低遭攻擊者入侵的風險。

4. 網路管理人員應參考最新威脅情資與受駭偵測指標，確實部署預防性阻擋措施，以攔截並過濾可疑郵件。
5. 建議各單位持續加強內部資安宣導與演練作業，提升人員對社交工程攻擊的辨識能力與防護意識，以降低遭駭風險。

2.3 軟硬體系統資安議題

2.3.1 關鍵 RCE 漏洞「React2Shell」遭大規模積極利用

Google 威脅情報小組（Google Threat Intelligence Group, GTIG）近日發布最高級別警報，指出編號 CVE-2025-55182 的遠端程式碼執行（RCE）漏洞已被攻擊者在實際環境中積極利用。這項被稱為 「React2Shell」 的漏洞影響主流前端框架 React 與 Next.js，其 CVSS v3.x 嚴重度評分達滿分 10.0，顯示風險極高並可能造成廣泛衝擊。

CVE-2025-55182 是一個極為嚴重的 RCE 漏洞，它允許未經身份驗證的遠端攻擊者，在缺乏適當輸入驗證和處理的應用程式環境中執行任意程式碼。

影響範圍廣泛：此漏洞主要衝擊 React 與 Next.js 的資料處理與渲染流程。由於 React 是全球最常用的前端框架，而 Next.js 又是其主流的服務端渲染（SSR）框架，因此相關應用的潛在受影響面積相當巨大。

攻擊方式：攻擊者可利用特定格式的惡意輸入觸發弱點，從而繞過既有的安全沙箱或資料清理機制，迫使伺服器執行惡意指令。成功攻擊後，攻擊者可能完全掌控伺服器，包括竊取資料、植入惡意程式（例如挖礦程式或後門），甚至將設備納入殭屍網路。

主要風險：漏洞之所以極具威脅性，在於其具備「遠端」與「零權限」攻擊特性，攻擊者無需取得任何帳號或進行複雜前置步驟即可入侵，大幅提高攻擊成功率並對企業資產造成直接衝擊。

GTIG 已確認多起針對 CVE-2025-55182 的攻擊事件，並在部分案例中觀察到攻擊者成功部署 XMRig 密碼貨幣礦工。GTIG 的調查顯示，至少有一起攻擊可明確歸因於其追蹤的駭客組織 UNC6584。此外，外部情資也顯示本次活動可能與另外兩個團體有關，分別為 UNC5454（Earth Lamia）與 UNC3569（Jackpot Panda）。然而，GTIG 目前的主要證據仍集中指向 UNC6584，其參與度最為明確。

目前網路上已存在多個功能性的合法遠端程式碼執行（RCE）利用程式碼。更重要的是，GTIG 觀察到先前被視為「虛假」的公開 PoC 程式碼庫正不斷被更新並加入真正的 RCE 攻擊能力，因此企業絕不應輕忽其當前威脅。GTIG 的監測活動，包括在 AWS 和 GreyNoise 蜜罐中掌握到的利用實例，證實了攻擊者正積極且實際地利用此漏洞。

建議企業應儘速完成漏洞更新，並同步強化防護與監控措施，以降低遭受攻擊的風險。以下提供主要因應建議：

1. 立即修補
   - 建議所有使用 React 的組織立即升級至 React 19.2.1。
   - 使用 Next.js 的環境應盡速更新至官方提供的最新修補版本。
2. Google Cloud 防護措施
   - Google Cloud 用戶可啟用新版 Cloud Armor WAF 規則 cve-canary，作為前線防護，減少遭受攻擊成功的風險。
3. 持續監控與威脅偵測
   - 建議安全團隊加強監控主機與服務紀錄，特別是檢查是否出現未經授權的 XMRig 部署、異常 CPU 使用率、可疑網路連線或其他可能的入侵跡象。

- 相關連結
  1. Responding to CVE-2025-55182: Secure your React and Next.js workloads
  2. React2Shell (CVE-2025-55182): Everything You Need to Know About the Critical React Vulnerability

2.4 軟硬體漏洞資訊

2.4.1 WordPress擴充程式與網頁主題存在6個安全漏洞

CVE 編號	CVE-2025-13536,CVE-2025-13538,CVE-2025-13539,CVE-2025-13540,CVE-2025-13615,CVE-2025-13675
影響產品	WordPress 擴充程式與網頁主題
解決辦法	更新 Blubrry PowerPress 至 11.15.3(含)以後版本 更新 FindAll Listing 至 1.1(含)以後版本 更新 FindAll Membership 至 1.1(含)以後版本 更新 Tiare Membership 至 1.3(含)以後版本 更新 StreamTube Core 至 4.79(含)以前後版本 Tiger 網頁主題請參考官方說明採取必要措施，網址如下： https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-themes/tiger-2/tiger-10121-unauthenticated-privilege-escalation

- 內容說明：

  研究人員發現 WordPress 擴充程式與網頁主題存在 6 個高風險安全漏洞，請儘速確認並進行修補。

  1. Blubrry PowerPress 擴充程式存在任意檔案上傳(Arbitrary File Upload)漏洞(CVE-2025-13536)，取得一般權限之遠端攻擊者可於受影響網頁伺服器上傳並執行網頁後門程式，進而達成遠端執行任意程式碼。

  2. FindAll Listing 與 Tiare Membership 擴充程式及 Tiger 網頁主題存在權限提升(Privilege Escalation)漏洞(CVE-2025-13538、CVE-2025-

13540 及 CVE-2025-13675)，未經身分鑑別之遠端攻擊可於註冊時指定管理者角色，進而利用漏洞取得網站管理員權限。

3. FindAll Membership 擴充程式存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2025-13539)，未經身分鑑別之遠端攻擊者於取得一般使用者帳號且能存取管理員電子郵件之情況下，可以管理員身分登入系統。

4. StreamTube Core 擴充程式存在任意使用者密碼變更(Arbitrary User Password Change)漏洞(CVE-2025-13615)，未經身分鑑別之遠端攻擊者可任意變更網站使用者密碼，進而取得管理員帳號權限。

- 影響平台：
  - Blubrry PowerPress 11.15.2(含)以前版本
  - FindAll Listing 1.0.5(含)以前版本
  - FindAll Membership 1.0.4(含)以前版本
  - Tiare Membership 1.2(含)以前版本
  - StreamTube Core 4.78(含)以前版本
  - Tiger 網頁主題 101.2.1(含)以前版本

- 資料來源：
  1. CVE-2025-13536
  2. CVE-2025-13538
  3. CVE-2025-13539
  4. CVE-2025-13540
  5. CVE-2025-13615
  6. CVE-2025-13675
  7. Blubrry PowerPress <= 11.15.2 - Authenticated (Contributor+) Arbitrary File Upload via 'powerpress_e
  8. FindAll Listing <= 1.0.5 - Unauthenticated Privilege Escalation
  9. FindAll Membership <= 1.0.4 - Authentication Bypass via Social Login
  10. Tiare Membership <= 1.2 - Unauthenticated Privilege Escalation
  11. StreamTube Core <= 4.78 - Unauthenticated Arbitrary User Password Change
  12. Tiger <= 101.2.1 - Unauthenticated Privilege Escalation

2.4.2 ASUS DSL路由器存在高風險安全漏洞(CVE-2025-59367)

CVE 編號	CVE-2025-59367
影響產品	ASUS DSL-AC51、DSL-AC750、DSL-N16
解決辦法	官方已針對漏洞釋出修復更新，請更新至以下版本： ASUS DSL-AC51 Firmware 1.1.2.3_1010 版本 ASUS DSL-AC750 Firmware 1.1.2.3_1010 版本 ASUS DSL-N16 Firmware 1.1.2.3_1010 版本 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.asus.com/security-advisory

- 內容說明：

  研究人員發現 ASUS 部分 DSL 型號路由器存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2025-59367)。

  未經身分鑑別之遠端攻擊者可透過此漏洞，對受影響設備執行未經授權之存取，請儘速確認並進行修補。

- 影響平台：
  - DSL-AC51
  - DSL-AC750
  - DSL-N16
- 資料來源：
  1. CVE-2025-59367
  2. ASUS Product Security Advisory

2.4.3 Fortinet FortiWeb存在高風險安全漏洞(CVE-2025-58034)

CVE 編號	CVE-2025-58034
影響產品	Fortinet FortiWeb
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://fortiguard.fortinet.com/psirt/FG-IR-25-513

- 內容說明：

  研究人員發現 Fortinet FortiWeb 存在作業系統指令注入(OS Command Injection)漏洞(CVE-2025-58034)。

  已取得管理權限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。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - FortiWeb 8.0.0 至 8.0.1 版本
  - FortiWeb 7.6.0 至 7.6.5 版本
  - FortiWeb 7.4.0 至 7.4.10 版本
  - FortiWeb 7.2.0 至 7.2.11 版本
  - FortiWeb 7.0.0 至 7.0.11 版本
- 資料來源：
  1. CVE-2025-58034
  2. Multiple OS command injection in API and CLI

2.4.4 Fortinet 旗下多項產品發布重大資安公告

CVE 編號	CVE-2025-59718,CVE-2025-59719
影響產品	Fortinet FortiOS、FortiProxy、FortiSwitchManager、FortiWeb
解決辦法	【CVE-2025-59718】 請更新至以下版本： FortiOS 7.6.4(含)之後版本、 FortiOS 7.4.9(含)之後版本、 FortiOS 7.2.12(含)之後版本、 FortiOS 7.0.18(含)之後版本、 FortiProxy 7.6.4(含)之後版本、 FortiProxy 7.4.11(含)之後版本、 FortiProxy 7.2.15(含)之後版本、 FortiProxy 7.0.22(含)之後版本、 FortiSwitchManager 7.2.7(含)之後版本、 FortiSwitchManager 7.0.6(含)之後版本 【CVE-2025-59719】 請更新至以下版本： FortiWeb 7.4.10(含)之後版本、 FortiWeb 7.6.5(含)之後版本、 FortiWeb 8.0.1(含)之後版本

- 內容說明：

  【CVE-2025-59718，CVSS：9.8】

  FortiOS、FortiProxy 及 FortiSwitchManager 存在繞過身分驗證漏洞，未經身分驗證的攻擊者可利用特製的 SAML 訊息，繞過 FortiCloud SSO 的身分驗證機制。

  【CVE-2025-59719，CVSS：9.8】

  FortiWeb 存在繞過身分驗證漏洞，未經身分驗證的攻擊者可利用特製的 SAML 訊息，繞過 FortiCloud SSO 的身分驗證機制。

- 影響平台：

  【CVE-2025-59718】

  - FortiOS 7.6.0 至 7.6.3 版本、
  - FortiOS 7.4.0 至 7.4.8 版本、
  - FortiOS 7.2.0 至 7.2.11 版本、
  - FortiOS 7.0.0 至 7.0.17 版本、
  - FortiProxy 7.6.0 至 7.6.3 版本、
  - FortiProxy 7.4.0 至 7.4.10 版本、
  - FortiProxy 7.2.0 至 7.2.14 版本、
  - FortiProxy 7.0.0 至 7.0.21 版本、
  - FortiSwitchManager 7.2.0 至 7.2.6 版本、
  - FortiSwitchManager 7.0.0 至 7.0.5 版本

  【CVE-2025-59719】

  - FortiWeb 7.4.0 至 7.4.9 版本、
  - FortiWeb 7.6.0 至 7.6.4 版本、
  - FortiWeb 8.0.0 版本

- 資料來源：

  1. Multiple Fortinet Products' FortiCloud SSO Login Authentication Bypass
  2. CVE-2025-59718
  3. CVE-2025-59719

2.4.5 Ivanti旗下EPM存在2個重大資安漏洞

CVE 編號	CVE-2025-10573,CVE-2025-13659
影響產品	Ivanti EPM
解決辦法	請更新至以下版本： EPM 2024 SU4 SR1 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。

  【CVE-2025-10573，CVSS：9.6】

  此為儲存型跨站腳本攻擊漏洞，允許遠端未經驗證的攻擊者在管理員工作階段中執行任意 JavaScript 程式碼。

  【CVE-2025-13659，CVSS：8.8】

  此為任意檔案寫入漏洞，因對動態管理的程式碼資源控制不當，使得遠端未經驗證的攻擊者能在伺服器上寫入任意檔案，並可能導致遠端程式碼執行。

- 影響平台：
  - EPM 2024 SU4(含)之前版本
- 資料來源：
  1. Security Advisory EPM December 2025 for EPM 2024
  2. CVE-2025-10573
  3. CVE-2025-13659

2.4.6 SAP針對旗下2款產品發布重大資安公告

CVE 編號	CVE-2025-42928,CVE-2025-42880
影響產品	SAP jConnect - SDK for ASE、SAP Solution Manager ST 720
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/december-2025.html

- 內容說明：

  【CVE-2025-42928，CVSS：9.1】

  此漏洞為反序列化漏洞，具備高權限的使用者可能利用此漏洞，觸發遠端程式碼執行攻擊，影響系統的機密性、完整性和可用性。

  【CVE-2025-42880，CVSS：9.9】

  由於缺乏輸入過濾機制，SAP Solution Manager 允許已驗證的攻擊者在呼叫支援遠端的功能模組時植入惡意程式碼，可能影響系統的機密性、完整性和可用性。

- 影響平台：

  【CVE-2025-42928】

  - SAP jConnect - SDK for ASE
    SYBASE_SOFTWARE_DEVELOPER_KIT 16.0.4, 16.1 版本

  【CVE-2025-42880】

  - SAP Solution Manager ST 720 版本

- 資料來源：

  1. SAP Security Patch Day - December 2025
  2. CVE-2025-42928
  3. CVE-2025-42880

2.4.7 Meta旗下React Server Components存在重大資安漏洞(CVE-2025-55182)

CVE 編號	CVE-2025-55182
影響產品	React Server Components
解決辦法	根據官方網站釋出的解決方式進行修補：https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

- 內容說明：

  React 是一個由 Meta 開發的開源 JavaScript 函式庫，用於建構使用者介面。近日 Meta 發布重大資安漏洞公告(CVE-2025-55182，CVSS：10.0)，指出 React Server Components 存在遠端程式碼執行漏洞。由於 React 在解析傳送至 React Server Function 端點的資料時存在安全弱點，攻擊者無需通過身分驗證，即可能透過特製有效負載觸發任意程式碼執行。

- 影響平台：
  - react-server-dom-webpack 19.0、19.1.0、19.1.1、19.2.0 版本
  - react-server-dom-parcel 19.0、19.1.0、19.1.1、19.2.0 版本
  - react-server-dom-turbopack 19.0、19.1.0、19.1.1、19.2.0 版本
  - 受影響的 React 框架與打包工具包括：next, react-router, waku, @parcel/rsc, @vitejs/plugin-rsc 及 rwsdk。
- 資料來源：
  1. CVE-2025-55182
  2. Critical Security Vulnerability in React Server Components
  3. CVE-2025-55182

2.4.8 Sangoma旗下電話管理系統FreePBX存在重大資安漏洞(CVE-2025-66039)

CVE 編號	CVE-2025-66039
影響產品	Sangoma FreePBX
解決辦法	請更新至以下版本： FreePBX 16.0.44 版本 FreePBX 17.0.23 版本

- 內容說明：

  FreePBX 是 Sangoma 旗下開源 IP 電話管理系統，包含管理網路電話、來電轉接、會議功能等。近期 FreePBX 發布重大資安公告，指出系統的模組 FreePBX Endpoint Manager 存在身分驗證錯誤漏洞(CVE-2025-66039，CVSS 4.x：9.3)，若身份驗證類型設定為「webserver」時，該模組存在身分驗證繞過漏洞；若 Authorization 標頭的值為任意，無論憑證是否有效，都會把 session 導向目標使用者。

- 影響平台：
  - FreePBX 16.0.44 版本(不含)之前版本
  - FreePBX 17.0.23 版本(不含)之前版本
- 資料來源：
  1. Security Advisories
  2. CVE-2025-66039

2.4.9 Cisco旗下AsyncOS軟體存在重大資安漏洞(CVE-2025-20393)

CVE 編號	CVE-2025-20393
影響產品	Cisco AsyncOS
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-sma-attack-N9bf4

- 內容說明：

  AsyncOS 軟體是 Cisco 專門設計用於 Cisco Secure Email Gateway、Cisco Secure Email 和 Web Manager 的作業系統，提供處理大量郵件與網路流量，提供進階的郵件安全等多項功能。Cisco 發布重大資安公告，發現 AsyncOS 存在重大資安漏洞(CVE-2025-20393，CVSS：10.0)，此漏洞允許攻擊者在受影響設備的底層系統以 root 權限執行任意命令，目前已被發現用於網路攻擊活動，詳細解決方案請見 Cisco 官網。

- 影響平台：
  - 所有版本的 Cisco AsyncOS 軟體均受此攻擊活動影響
- 資料來源：
  1. Reports About Cyberattacks Against Cisco Secure Email Gateway And Cisco Secure Email and Web Manager
  2. CVE-2025-20393
  3. CVE-2025-20393

2.4.10 WatchGuard Firebox存在重大資安漏洞(CVE-2025-14733)

CVE 編號	CVE-2025-14733
影響產品	WatchGuard Firebox
解決辦法	請更新至以下版本： WatchGuard Fireware OS 2025.1.4 版本、 WatchGuard Fireware OS 12.5.15 版本、 WatchGuard Fireware OS 12.11.6 版本、 WatchGuard Fireware OS 12.3.1_Update4 (B728352)版本 備註：WatchGuard Fireware OS 11.x 版本已是 EoL(End of Life)的產品，建議升級至支援版本

- 內容說明：

  WatchGuard Firebox 是一款次世代防火牆產品，提供多層次防護，包括防毒、IPS、APT 阻擋及垃圾郵件過濾。WatchGuard 發布重大資安漏洞(CVE-2025-14733，CVSS 4.x：9.3)公告，該漏洞為越界寫入漏洞，可能允許遠端未經驗證的攻擊者執行任意程式碼，目前 WatchGuard 已觀察到攻擊者正積極嘗試利用此漏洞，詳細說明請見 WatchGuard 官網。

- 影響平台：
  - WatchGuard Fireware OS 2025.1 至 2025.1.3 版本
  - WatchGuard Fireware OS 12.5 至 12.5.14 版本
  - WatchGuard Fireware OS 12.0 至 12.11.5 版本
  - WatchGuard Fireware OS 11.10.2.至 11.12.4+541730 版本
- 資料來源：
  1. WatchGuard Firebox iked Out of Bounds Write Vulnerability
  2. CVE-2025-14733

2.4.11 WordPress擴充程式與網頁主題存在10個高風險安全漏洞

CVE 編號	CVE-2025-67522,CVE-2025-67523,CVE-2025-67524,CVE-2025-67525,CVE-2025-67526,CVE-2025-67527,CVE-2025-67529,CVE-2025-67530,CVE-2025-67531,CVE-2025-67532
影響產品	WordPress 擴充程式與網頁主題
解決辦法	請更新至以下版本： Jobmonster Elementor Addon 1.1.5(含)以後版本 Jobmonster 4.8.3(含)以後版本 Exhibz 3.0.10(含)以後版本 ekommart 4.3.1(含)以後版本 Sailing 4.4.6(含)以後版本 Digiqole 2.2.7(含)以後版本 Fashion 5.3.0(含)以後版本 Besa 2.3.16(含)以後版本 Turitor 1.5.3(含)以後版本 Hara 1.2.18(含)以後版本

- 內容說明：

  研究研究人員發現 WordPress 擴充程式與網頁主題存在 PHP 本機檔案包含(PHP Local File Inclusion)漏洞(CVE-2025-67522、CVE-2025-67523、CVE-2025-67524、CVE-2025-67525、CVE-2025-67526、CVE-2025-67527、CVE-2025-67529、CVE-2025-67530、CVE-2025-67531 及 CVE-2025-67532)。未經身分鑑別之遠端攻擊者可利用此漏洞，誘使伺服器端 PHP 程式載入本機非預期檔案，並於伺服器端執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - Jobmonster Elementor Addon 1.1.4(含)以前版本
  - Jobmonster 4.8.2(含)以前版本
  - Exhibz 3.0.9(含)以前版本
  - ekommart 4.3.1(不含)以前版本
  - Sailing 4.4.6(不含)以前版本
  - Digiqole 2.2.7(不含)以前版本
  - Fashion 5.3.0(不含)以前版本
  - Besa 2.3.15(含)以前版本
  - Turitor 1.5.3(不含)以前版本
  - Hara 1.2.17(含)以前版本
- 資料來源：
  1. CVE-2025-67522
  2. CVE-2025-67523
  3. CVE-2025-67524
  4. CVE-2025-67525
  5. CVE-2025-67526
  6. CVE-2025-67527
  7. CVE-2025-67529
  8. CVE-2025-67530
  9. CVE-2025-67531
  10. CVE-2025-67532

2.4.12 Zimbra旗下Zimbra Collaboration Suite存在重大資安漏洞(CVE-2025-68645)

CVE 編號	CVE-2025-68645
影響產品	Zimbra Collaboration Suite
解決辦法	根據官方網站釋出解決方式進行修補。

- 內容說明：

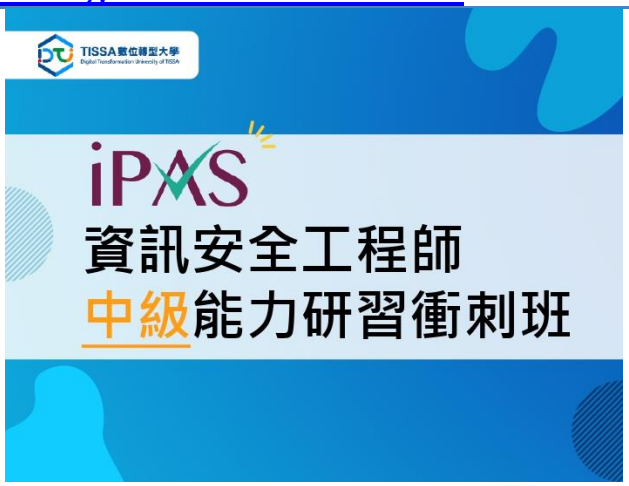
  郵件伺服器系統 Zimbra Collaboration Suite 的 Webmail Classic UI 中存在重大本機檔案包含漏洞(Local File Inclusion，LFI)，漏洞編號為 CVE-2025-68645(CVSS：8.8)。該漏洞源於 RestFilter Servlet 對使用者提供的請求參數處理不當，未經身分驗證的遠端攻擊者可對 /h/rest 端點請求，從而影響內部請求分發，包含 WebRoot 目錄中的任意檔案。

- 影響平台：
  - Zimbra Collaboration Suite 10.0 版本
  - Zimbra Collaboration Suite 10.1 版本
- 資料來源：
  1. Zimbra Security - News & Alerts
  2. Zimbra Daffodil 10.0.18 Patch Release
  3. Zimbra Daffodil (v10.1.13) Patch Release
  4. CVE-2025-68645

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** **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：

立即科技｜企業雲端資料庫 - Hard-coded Cryptographic Key	
TVN / CVE ID	TVN-202512007 / CVE-2025-15016
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	企業雲端資料庫
問題描述	企業雲端資料庫存在Hard-coded Cryptographic Key漏洞，未經身分鑑別之遠端攻擊者可利用固定key產生驗證資訊，進而以任意使用者身分登入系統。
解決方法	聯繫廠商安裝修補程式
公開日期	2025-12-22
相關連結	https://www.twcert.org.tw/tw/cp-132-10587-797c6-1.html
旭聯科技｜WMPro 智慧大師 - Arbitrary File Upload	
TVN / CVE ID	TVN-202512008 / CVE-2025-15226
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	WMPro 5.0至5.2版本
問題描述	CVE-2025-15226： WMPro智慧大師存在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	聯繫廠商安裝修補程式並調整系統設定
公開日期	2025-12-29

相關連結	**https://www.twcert.org.tw/tw/cp-132-10602-c1c69-1.html**
鴻名企業北專案技術部｜BPMFlowWebkit - Arbitrary File Upload	
TVN / CVE ID	TVN-202512009 / CVE-2025-15228
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	BPMFlowWebkit 5.0.5(不含)以前版本
問題描述	CVE-2025-15228： BPMFlowWebkit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	請更新至5.0.5(含)以後版本
公開日期	2025-12-29
相關連結	**https://www.twcert.org.tw/tw/cp-132-10604-c65aa-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12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/**