TWCERT/CC 資安情資電子報

2025 年 8 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

半導體戰略背後的網路戰–資安攻擊鎖定設計、生產與財經分析師

美國資安公司 Proofpoint 最新揭露，三個與中國有關聯的駭客組織於 2025 年 3 月至 6 月間，針對台灣半導體產業發動大規模網路攻擊。Proofpoint 在尚未經長期觀察以確認身份前，會將疑似進階持續性威脅（APT）組織以「UNK」為前綴命名，待身份確立後則改為「TAG」。本次行動涉及的三個主要駭客組織分別為 UNK_DropPitch、UNK_SparkyCarp 與 UNK_FistBump。報告顯示，過去中國駭客行動多

集中在國防、政府及學術研究領域，但此次攻擊的規模與集中程度顯示，其戰略重心已轉向以台灣主要晶圓代工企業為核心的半導體生態系統，目標可能在於取得先進製程技術，或干擾針對中國的技術封鎖應對策略。

根據 Proofpoint 與開源威脅情報分析，攻擊者主要透過魚叉式釣魚（spear-phishing）郵件，並利用擬真的履歷表、產業報告、薪資資訊或投資分析內容作為誘餌文件，鎖定台灣半導體公司內部的工程師、人資與財經分析師，一旦受害者開啟附檔或點擊連結，便可在目標電腦中植入多種遠端控制工具，包括 Cobalt Strike beacon 與罕見的 Voldemort 後門程式，以維持長期潛伏並竊取敏感資料，實施間諜行為。Proofpoint 進一步指出，UNK_DropPitch駭客組織更將攻擊範圍擴及研究機構與金融投資顧問，推測其意圖為掌握台灣晶片企業的未來動態與商業機密，對產業機密與供應鏈安全構成重大威脅。

UNK_FistBump於2025年5月至6月間入侵台灣大學研究生的電子郵件帳號，並冒用其身份向台灣半導體製造、封裝、測試及供應鏈相關企業的人力資源部門寄送多封釣魚郵件，偽稱為求職者以引誘收件人開啟附件，如圖1所示。這些郵件附件包含指向 Zendesk 或 Filemail 等線上檔案共享服務的連結，所存放的檔案為惡意程式，包括 Cobalt Strike Beacon 與罕見的 Voldemort 後門程式。根據 Proofpoint 分析，不同惡意程式所觸發的攻擊鏈有所差異，顯示該組織具備針對不同目標進行攻擊手法調整的能力，如圖2所示。

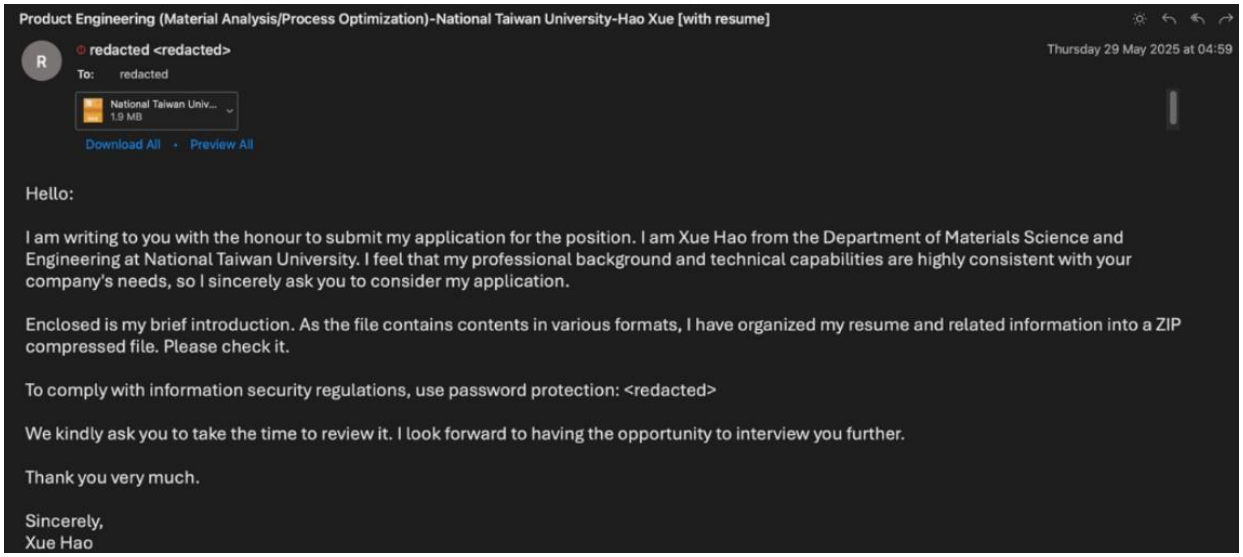

圖1：UNK_FistBum使用的求職釣魚電子郵件。圖片來源：Proofpoint

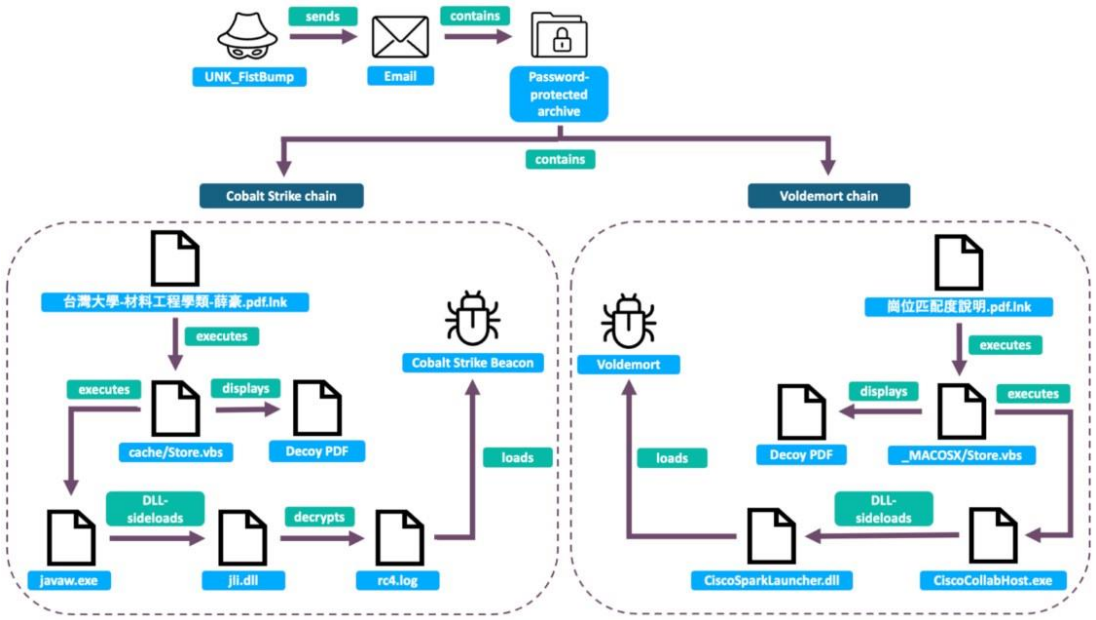

圖2：UNK_FistBum所使用的惡意程式流程圖。圖片來源：Proofpoint

2025年4月至5月間，UNK_DropPitch駭客組織針對多家大型投資銀行發動網路釣魚攻擊，鎖定專門從事台灣半導體與科技產業金融投資分

析的分析師。攻擊者偽裝成虛構的金融投資公司，聲稱欲與目標合作投資，並透過釣魚郵件引誘受害者開啟附件，如圖3所示。

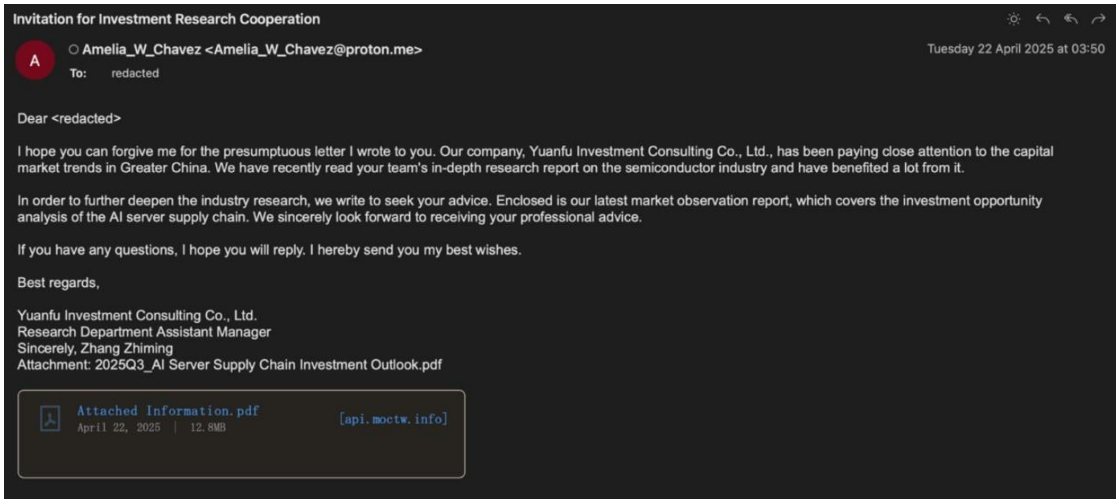

圖3：UNK_DropPitch使用的尋求投資合作釣魚電子郵件。圖片來源：Proofpoint

釣魚郵件內的附檔連結指向 api[.]moctw[.]info，疑似偽造成「中華民國交通部」（Ministry of Transportation and Communications, R.O.C.，簡稱 MOTC 或 MoTC）或「文化部」（Ministry of Culture，MoC）的官方 API 端點，以提高可信度，誘使受害者相信此API是政府授權服務。當受害者點擊連結，將下載含惡意libcef.dll 檔案的壓縮包，該DLL作為加載器，用於載入HealthKick後門程式。

此外，Proofpoint 亦觀察到該組織使用另一個C2：brilliant-bubblegum-137cfe[.]netlify[.]app，該平台為Netlify提供合法的免費靜態網站服務，但經常被濫用於 C2、釣魚或惡意檔案託管。在此事件手法中，攻擊者透過該域名投遞另一個名為pbvm90.dll的惡意DLL作為加載器，展現其靈活運用多種基礎設施與載荷的能力。

UNK_SparkyCarp駭客組織於2025年3月針對一家台灣半導體公司發動網路釣魚攻擊。該組織架設兩個 C2 網域 accshieldportal[.]com與

acesportal[.]com，並偽造登入頁面以模仿企業內部系統，試圖誘使受害員工輸入帳號與密碼，以竊取憑證資訊，如圖4所示。攻擊行動顯示 UNK_SparkyCarp 在基礎設施佈署上具備針對性與客製化能力，並以高仿真的社交工程手法提升攻擊成功率。

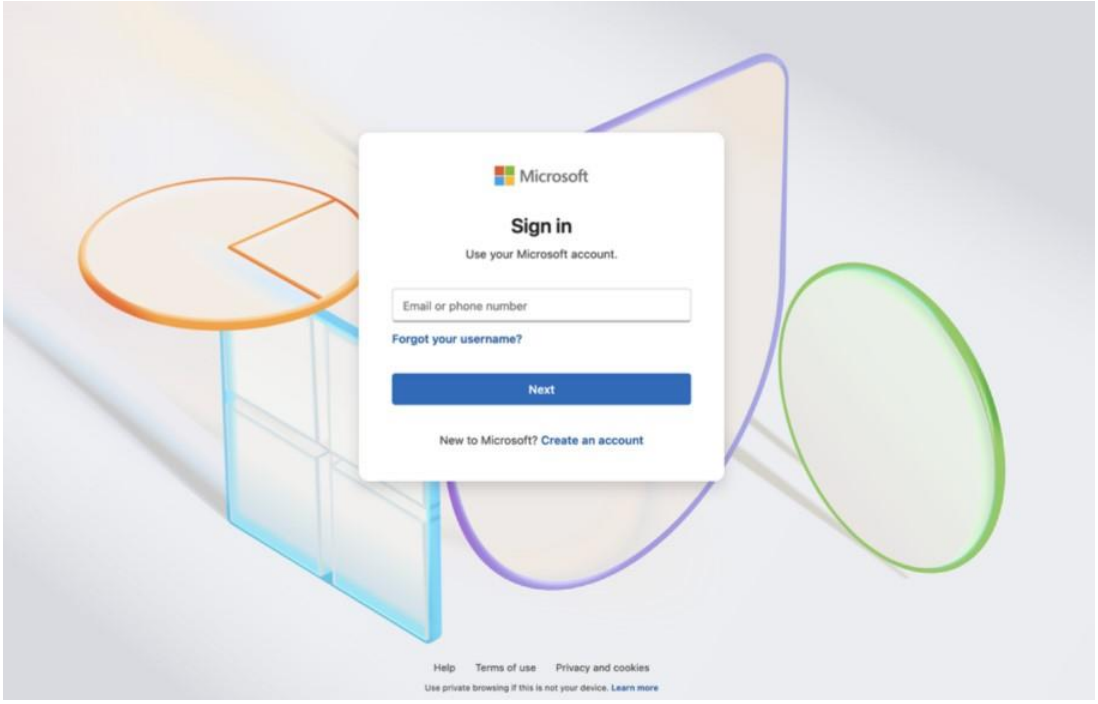

圖4 : UNK_SparkyCarp使用釣魚網站。圖片來源：Proofpoint

TWCERT/CC根據上述內容整理成以下表格：

項目	UNK_FistBump	UNK_DropPitch	UNK_SparkyCarp
攻擊時間	2025 / 05 - 2025 / 06	2025 / 04 - 2025 / 05	2025 / 03
攻擊初始方式	釣魚郵件	釣魚郵件	釣魚郵件
攻擊目標	台灣半導體公司	台灣半導體產業分析師	台灣半導體公司
釣魚信寄件者	入侵台大學生帳號	偽冒投資公司	-
惡意程式託管/使用的 C2	Zendesk、Filemail	api[.]moctw[.]info、brilliant-bubblegum-137cfe[.]netlify[.]app	accshieldportal[.]com、acesportal[.]com
使用的惡意程	Voldemort、Cobalt Strike Beacon	HealthKick	-

式			
使用的惡意 DLL 名稱	-	libcef.dll、pbvm90.dll	-
攻擊目的	-	-	獲取員工帳號密碼

- 相關連結
  1. Chinese Hackers Target Taiwan's Semiconductor Sector with Cobalt Strike, Custom Backdoors
  2. Phish and Chips: China-Aligned Espionage Actors Ramp Up Taiwan Semiconductor Industry Targeting

第 2 章、國內外重要資安事件

2.1 軟體系統資安議題

2.1.1 駭客利用SonicWall裝置植入「隱形後門」，恐長期竊取組織機密

Google威脅情報小組（GTIG）揭露一個被名為「UNC6148」的駭客組織。對SonicWall網路安全設備（SMA100系列）展開攻擊。即使設備已經安裝官方的更新修補，駭客仍能利用先前竊取的管理憑證和一次性密碼（OTP）重新取得權限，顯示這次攻擊具針對性與隱蔽性。

資安公司Mandiant調查發現，駭客組織已掌握目標設備的本地管理員憑證，然而，這些憑證取得方式仍未知。根據SonicWall公布的韌體修補時間表與針對漏洞的公開報告，GTIG推測駭客組織可能利用漏洞在

目標設備更新前竊取管理員憑證。

來自SonicWall和資安業界的報告指出，UNC6148可能利用以下幾項漏洞：

- CVE-2021-20038 (CVSS:9.8)為堆疊緩衝區溢位漏洞，允許未經身分驗證的遠端攻擊者執行程式碼。
- CVE-2024-38475 (CVSS:9.1)是Apache HTTP Server 存在未經驗證的路徑遍歷漏洞，影響SAM 100系列設備。watchTowr曾揭露該漏洞與CVE-2023-44221可組合成攻擊鏈。目前尚未有證據表明UNC6148使用此漏洞鏈。
- CVE-2021-20035 (CVSS:6.5)和CVE-2021-20039 (CVSS:8.8)皆為命令注入漏洞，允許經過身分驗證的遠端攻擊者注入任意命令。
- CVE-2025-32819 (CVSS:8.8)允許具有SSLVPN使用者權限的遠端攻擊者，繞過路徑遍歷保護機制，刪除任意系統檔案。

一旦駭客組織入侵 SonicWall SMA100系列設備，就會植入一個名為「OVERSTEP」的惡意程式。這是一種專為SonicWall SMA100系列設備設計的C語言後門程式，能在設備重新開機後持續運作，並可與駭客伺服器建立反向連線（反向 shell），竊取企業內部帳號、密碼與憑證等敏感資料，甚至進一步發動勒索攻擊。為了躲避偵測，OVERSTEP還會偽裝成系統檔案、刪除系統日誌與攻擊紀錄，使資安人員難以追蹤其入侵行為。

目前已知的受害企業及組織範圍廣泛，包括中小企業、政府機關、醫療機構等。GTIG 發現，有些企業在被駭後，其機密資料甚至被公開在「World Leaks」網站。此外，該駭客組織與部署Abyss勒索病毒有關聯，說明攻擊目的不只是竊取資料，還可能發展成勒索行動。

這次的攻擊活動不像一般駭客入侵，是一場精心策劃且持續滲透的高階攻擊。即使設備已更新，駭客仍能利用過去竊取的憑證和密碼重新入侵。一旦被攻擊，整個組織和合作夥伴都可能受到影響。GTIG 建議：

- 立即檢查是否使用 SonicWall SMA 100 系列設備
- 重新設定所有密碼與一次性密碼（OTP）
- 更換裝置上的所有憑證與私鑰
- 檢查系統日誌是否有異常或可疑程式執行
- 必要時尋求SonicWall或資安公司協助，執行數位鑑識分析

● 相關連結

1. Ongoing SonicWall Secure Mobile Access (SMA) Exploitation Campaign using the OVERSTEP Backdoor
2. UNC6148 Backdoors Fully-Patched SonicWall SMA 100 Series Devices with OVERSTEP Rootkit
3. SonicWall SMA devices persistently infected with stealthy OVERSTEP backdoor and rootkit

2.1.2 Outlook「一鍵後門」一年後仍未封堵！Specula 框架持續威脅企業資安

2024 年公開的 Specula 框架，原本被視為紅隊測試的經典案例，如今在一年後依然可行。研究顯示，微軟雖已在 2017 年修補 CVE-2017-11774 (CVSS：7.8)，並移除 Outlook Home Page UI 選項，但核心功能並未完全封鎖。只要修改單一登錄檔值，攻擊者即可重新啟用，讓 Outlook 成為隱蔽的 C2 後門。

資安公司 TrustedSec 研究員 Oddvar Moe 在 2024 年公開 Specula C2 框架，示範如何透過 Outlook 的「Home Page」功能將郵件用戶端轉化為命令與控制（C2）通道。他指出，只要在 Windows 登錄檔新增 EnableRoamingFolderHomepages=1，並設定特定的 WebView URL，

Outlook 就會自動載入遠端 HTML 頁面並執行 VBScript。即使漏洞早已修補，這項技巧在 2025 年 7 月的一個研討會主題中《Redteam Chronicles: A C2 Story – Outlook's One-Setting Wonder》仍被證實能在大型企業的滲透測試中成功運用，顯示微軟並未徹底封鎖該功能。而資安公司 Mandiant 也曾觀察到 APT 團體（如 UNC1194）利用過類似的 Outlook Home Page 技術，凸顯這並非單純的研究展示，而是真實存在的威脅模式。

微軟當初設計此功能，是為了讓企業能將 SharePoint 等網站整合至 Outlook 主畫面。然而，研究人員發現，只要修改登錄檔，即可在沒有系統管理員權限的情況下重新啟用該功能，讓 Outlook 自動載入遠端 HTML 頁面並執行指令(如圖1)。

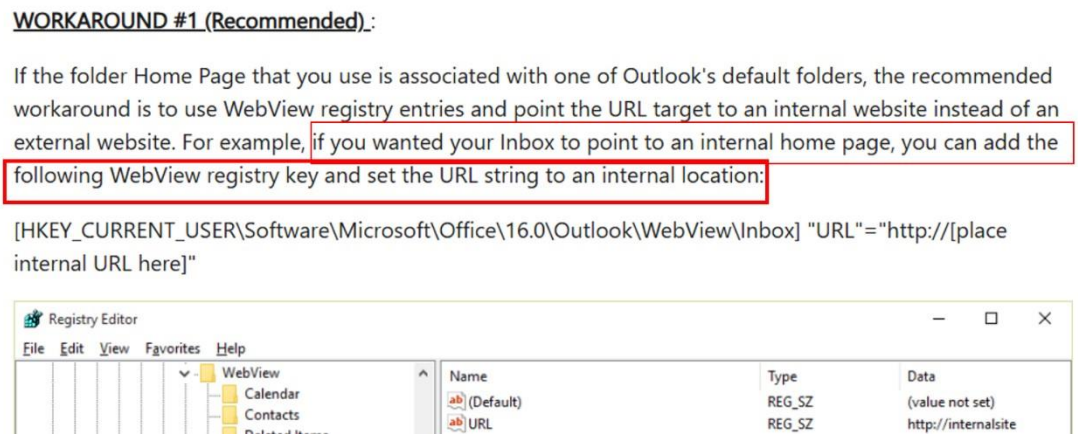

圖1：重新啟動漏洞，圖片來源：微軟官方文件

Moe 表示，團隊在多次紅隊演練與滲透測試中成功運用此手法，證明這項攻擊途徑依然存在。他強調：「我們不是為了炫技，而是要提醒產業界，這樣的攻擊依舊有效。只要微軟沒有徹底移除，紅隊與攻擊者就會繼續使用。」

雖然微軟已逐步淘汰 VBScript（Windows 11 24H3 可手動移除，預計 2027 年才全面停用），但尚未徹底封鎖 Home Page/WebView 功能。

因此，Specula 框架在 2025 年仍能被用來建立隱密的 C2 通道

在防禦層面，可採取以下緩解措施：

1. 在 Windows 11 24H3 版本起，使用者可選擇移除 VBScript，並預計於2027年全面預設移除。
2. 建議升級至新版 Outlook，避免使用舊版，降低被 Home Page/WebView 功能濫用的風險。
3. 可透過群組原則或自訂腳本，防止 URL 設定遭到竄改。
4. 監控登錄檔的變更，例如以下路徑中的 URL 欄位：
   - HKCU\Software\Microsoft\Office\\Outlook\WebView\Inbox
   - HKCU\Software\Microsoft\Office\
   - HKCU\Software\Microsoft\Office\

這項研究提醒企業：即便舊漏洞已經修補，官方文件中保留的啟用方式仍可能成為隱密後門。企業必須持續強化系統防護與監控，以避免類似攻擊再度發生。

- 相關連結
  1. Oddvar Moe: Redteam Chronicles: A C2 Story - Outlook's One-Setting Wonder
  2. Oddvar Moe: Redteam Chronicles: A C2 Story - Outlook's One-Setting Wonder
  3. Outlook Home Page feature is missing in folder properties
  4. Specula – Initial Install and Setup (Video 1)
  5. Github – trustedsec/specula

2.2 軟硬體漏洞資訊

2.2.1 趨勢科技旗下Apex One管理控制台存在2個重大資安漏洞

CVE 編號	CVE-2025-54948,CVE-2025-54987
影響產品	Trend Micro Apex One
解決辦法	根據官方網站釋出解決方式進行修補： https://success.trendmicro.com/en-US/solution/KA-0020652

- 內容說明：

  Apex One 是趨勢科技旗下一款端點安全整合式方案，提供集中式管理功能，可有效防護企業端點免受各種網路安全威脅侵害。日前，趨勢科技發布 2 個重大資安漏洞(CVE-2025-54948，CVSS：9.4 和 CVE-2025-54987，CVSS：9.4)，皆屬於作業系統指令注入漏洞，允許預授權的遠端攻擊者上傳惡意程式碼並執行命令。

- 影響平台：
  - Apex One (on-prem) 2019 14.0.0.14039(含)之前版本
- 資料來源：
  1. Trend Micro Apex One™ (On-Premise) Management Console Command Injection RCE Vulnerabilities
  2. CVE-2025-54948
  3. CVE-2025-54987

2.2.2 Adobe Experience Manager (JEE) 存在重大資安漏洞(CVE-2025-54253)

CVE 編號	CVE-2025-54253
影響產品	Adobe Experience Manager (JEE)
解決辦法	更新 Adobe Experience Manager (AEM) Forms on JEE 至 6.5.0-0108 版本

- 內容說明：

  Adobe 針對 Java 企業版(JEE)的 Adobe Experience Manager Forms 發布重大資安漏洞(CVE-2025-54253，CVSS：10.0)，此漏洞源於配置錯誤，攻擊者可利用此漏洞繞過安全機制並執行任意程式碼。

- 影響平台：
  - Adobe Experience Manager(AEM)Forms on JEE 6.5.23.0(含)之前版本
- 資料來源：
  1. Security updates available for Adobe Experience Manager Forms | APSB25-82
  2. CVE-2025-54253

2.2.3 Microsoft Exchange Server 存在重大資安漏洞(CVE-2025-53786)

CVE 編號	CVE-2025-53786
影響產品	Microsoft Exchange Server
解決辦法	根據官方網站釋出解決方式進行修補： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53786

- 內容說明：

  微軟針對旗下產品 Exchange Server 發布重大資安漏洞公告(CVE-2025-53786，CVSS：8.0)，此漏洞允許取得管理者權限的攻擊者，針對雲地混合部署的環境提升權限。目前雲端環境的日誌監控工具無法紀錄此漏洞的惡意活動。

  該漏洞相關 PoC 已於近日在美國黑帽大會 (Black Hat) 公開展示，可能加速攻擊者的後續利用，Microsoft 已釋出安全性更新與提供暫時緩解措施，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 Exchange Server Subion Edition RTM 15.02.0.0 至 15.02.2562.017 版本
  - Microsoft Exchange Server 2016 Cumulative Update 23 15.01.0 至 15.01.2507.055 版本
  - Microsoft Exchange Server 2019 Cumulative Update 14 15.02.0.0 至 15.02.1544.025 版本
  - Microsoft Exchange Server 2019 Cumulative Update 15 15.02.0 至 15.02.1748.024 版本

- 資料來源：
  1. Microsoft Exchange Server Hybrid Deployment Elevation of Privilege Vulnerability
  2. Microsoft Releases Guidance on High-Severity Vulnerability (CVE-2025-53786)
  3. CVE-2025-53786

2.2.4 Fortinet旗下FortiSIEM存在重大資安漏洞(CVE-2025-25256)

CVE 編號	CVE-2025-25256
影響產品	FortiSIEM
解決辦法	請更新至以下版本： FortiSIEM 7.3.2 版本 FortiSIEM 7.2.6 版本 FortiSIEM 7.1.8 版本 FortiSIEM 7.0.4 版本 FortiSIEM 6.7.10 版本 FortiSIEM 6.6(含)以下版本遷移至固定版本

- 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-2025-25256，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，透過精心設計的命令列介面(CLI)請求，執行未經授權的程式碼或命令。

- 影響平台：
  - FortiSIEM 7.3.0 至 7.3.1 版本
  - FortiSIEM 7.2.0 至 7.2.5 版本
  - FortiSIEM 7.1.0 至 7.1.7 版本
  - FortiSIEM 7.0.0 至 7.0.3 版本
  - FortiSIEM 6.7.0 至 6.7.9 版本
- 資料來源：
  1. Remote unauthenticated command injection
  2. CVE-2025-25256

2.2.5 Windows版Zoom用戶端存在重大資安漏洞(CVE-2025-49457)

CVE 編號	CVE-2025-49457
影響產品	Zoom
解決辦法	根據官方網站釋出解決方式進行修補： https://www.zoom.com/en/trust/security-bulletin/zsb-25030/?lang=null&lang=null

- 內容說明：

  Zoom 是一款跨平台雲端視訊會議軟體，支持多人線上會議、螢幕分享及會議錄製，適用於遠距工作與教學。Zoom 日前發布重大資安漏洞公告(CVE-2025-49457，CVSS：9.6)，部分 Windows 版 Zoom 客戶端存在不受信任的搜尋路徑漏洞，可能允許未經身分驗證的攻擊者，透過網路存取進行權限提升攻擊。

- 影響平台：
  - Zoom Workplace for Windows 6.3.10 之前版本
  - Windows 6.3.10 之前版本（6.1.16 和 6.2.12 除外）的 Zoom Workplace VDI
  - Windows 版 Zoom Rooms 6.3.10 之前版本
  - Windows 的 Zoom Rooms 控制器 6.3.10 之前版本
  - Windows 版 Zoom Meeting SDK 6.3.10 之前版本
- 資料來源：
  1. Zoom Clients for Windows - Untrusted Search Path
  2. CVE-2025-49457

2.2.6 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2025-42957,CVE-2025-42950,CVE-2025-42951
影響產品	SAP S/4HANA、Landscape Transformation、Business One
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/august-2025.html

- 內容說明：

  【CVE-2025-42957，CVSS：9.9】

  此漏洞存在於 SAP S/4HANA 和 SAP SCM Characteristic Propagation，允許具有使用者權限的攻擊者利用 RFC 公開功能模組的漏洞，將任意 ABAP 程式碼注入系統，從而繞過必要的授權檢查。

  【CVE-2025-42950，CVSS：9.9】

  該漏洞存在於 SAP Landscape Transformation (SLT)，允許具有使用者權限的攻擊者透過 RFC 公開功能模組的漏洞，將任意 ABAP 程式碼注入系統，從而繞過必要的授權檢查。

  【CVE-2025-42951，CVSS：8.8】

  SAP Business One (SLD) 存在授權漏洞，允許經過驗證的攻擊者透過呼叫對應的 API 取得資料庫的管理員權限。

- 影響平台：
  - SAP S/4HANA (Private Cloud or On-Premise) S4CORE 102, 103, 104, 105, 106, 107, 108 版本
  - SAP Landscape Transformation (Analysis Platform) DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 版本
  - SAP Business One (SLD) B1_ON_HANA 10.0, SAP-M-BO 10.0 版本

- 資料來源：
  1. SAP Security Patch Day - August 2025
  2. CVE-2025-42957
  3. CVE-2025-42950
  4. CVE-2025-42951

2.2.7 Cisco 旗下防火牆系統存在重大資安漏洞(CVE-2025-20265)

CVE 編號	CVE-2025-20265
影響產品	Cisco Secure Firewall Management Center
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-fmc-radius-rce-TNBKf79

- 內容說明：

  Cisco Secure Firewall Management Center（FMC）是一套集中式管理平台，用於統一管理與監控 Cisco 防火牆產品，提供完整的威脅防禦視野，並支援政策制定、事件分析、流量監控與裝置設定等功能。Cisco 發布重大資安漏洞公告(CVE-2025-20265，CVSS：10.0)並釋出更新版本，此漏洞存在於該透過 RADIUS 進行身份驗證時，允許未經身份驗證的遠端攻擊者注入任意 Shell 指令並使該裝置執行指令。

- 影響平台：
  - Cisco Firewall Management Center（FMC） 7.0.7、7.7.0 版本且已啟用 RADIUS 認證
- 資料來源：
  1. Cisco Secure Firewall Management Center Software RADIUS Remote Code Execution Vulnerability

2.2.8 Docker Windows版存在SSRF漏洞(CVE-2025-9074)

CVE 編號	CVE-2025-9074
影響產品	Docker Desktop
解決辦法	更新至 Docker Desktop 4.44.3(含)之後版本

- 內容說明：

  Docker Windows 桌機版是一款在 Windows 系統上運行的容器管理工具，透過容器技術簡化應用部署與管理。Docker 發布重大資安漏洞更新公告(CVE-2025-9074，CVSS 4.x：9.3)並釋出更新版本，此為伺服器請求偽造(SSRF)漏洞，允許攻擊者利用API執行各種特權指令，包括控制其他容器、管理映像等，此外，該漏洞還允許與執行Docker Desktop 的使用者以相同的權限掛載主機磁碟機。

- 影響平台：
  - Docker Desktop 4.44.3(不含)之前版本
- 資料來源：
  1. Docker Desktop release notes
  2. CVE-2025-9074

2.2.9 Commvault 存在重大資安漏洞(CVE-2025-57790)

CVE 編號	CVE-2025-57790
影響產品	Commvault
解決辦法	更新至 Commvault 11.32.102 (含)之後版本、Commvault 11.36.60 (含)之後版本

- 內容說明：

  備份與資料保護軟體廠商 CommVault，以企業級整合資料管理解決方案著稱，支援多平台、多環境的備份與還原，並提供高效的資料保護技術及雲端整合能力。近期發布重大資安漏洞公告(CVE-2025-57790，CVSS 3.x：8.8)，此漏洞允許遠端攻擊者利用路徑遍歷執行未經授權的檔案系統存取，可能導致遠端程式碼執行。

- 影響平台：
  - Commvault 11.32.0 至 11.32.101 版本
  - Commvault 11.36.0 至 11.36.59 版本
- 資料來源：
  1. CV_2025_08_2: Path Traversal Vulnerability
  2. CVE-2025-57790

2.2.10 Citrix旗下NetScaler ADC 和 NetScaler Gateway 存在2個重大資安漏洞

CVE 編號	CVE-2025-7775,CVE-2025-7776
影響產品	Citrix NetScaler ADC、NetScaler Gateway
解決辦法	請更新至以下版本： NetScaler ADC 和 NetScaler Gateway 14.1-47.48 (含)之後版本 NetScaler ADC 和 NetScaler Gateway 13.1-59.22 (含)之後版本 NetScaler ADC 13.1-FIPS 與 NDcPP 13.1-37.241-FIPS 與 NDcPP (含)之後版本 NetScaler ADC 12.1-FIPS 與 NDcPP 12.1-55.330-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。Citrix 發布重大資安漏洞公告(CVE-2025-7775，CVSS 4.x：9.2 和 CVE-2025-7776，CVSS 4.x：8.8)，CVE-2025-7775 為記憶體溢位漏洞，導致遠端程式碼或 DoS 攻擊；CVE-2025-7776 為記憶體溢位漏洞，導致不可預測或錯誤行為和 DoS 攻擊。

  另外，CVE-2025-7775 目前已觀察到有攻擊者利用，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。

  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 14.1-47.48 (不含)之前版本
  - NetScaler ADC 和 NetScaler Gateway 13.1-59.22 (不含)之前版本
  - NetScaler ADC 13.1-FIPS 與 NDcPP 13.1-37.241-FIPS 與 NDcPP (不含)之前版本
  - NetScaler ADC 12.1-FIPS 與 NDcPP 12.1-55.330-FIPS 與 NDcPP (不含)之前版本
- 資料來源：
  1. NetScaler ADC and NetScaler Gateway Security Bulletin
  2. CVE-2025-7775
  3. CVE-2025-7776

第 3 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：

二一零零科技｜公文管理系統 - Authentication Bypass	
TVN / CVE ID	TVN-202508001 / CVE-2025-8853
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	公文管理系統 5.0.89.0、5.0.89.1及5.0.89.2版本
問題描述	二一零零科技開發之公文管理系統存在Authentication Bypass漏洞，未經身分鑑別之遠端攻擊者可繞過限制取得任意使用者連線Token，並利用取得的Token以該使用者身分登入系統。
解決方法	更新至5.0.90(含)以後版本
公開日期	2025-08-11
相關連結	**https://www.twcert.org.tw/tw/cp-132-10319-adc18-1.html**
葳橋資訊｜單一簽入暨電子目錄服務系統 - Local File Inclusion	
TVN / CVE ID	TVN-202508002 / CVE-2025-8913
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	單一簽入暨電子目錄服務系統 IFTOP_P3_2_1_196(含)以前版本
問題描述	葳橋資訊開發之單一簽入暨電子目錄服務系統存在Local File Inclusion漏洞，未經身分鑑別之遠端攻擊者可利用此漏洞於伺服器端執行任意程式碼。
解決方法	更新至IFTOP_P3_2_1_197(含)以後版本

公開日期	2025-08-13
相關連結	**https://www.twcert.org.tw/tw/cp-132-10321-3cae5-1.html**
凱發科技｜WebITR - Missing Authentication	
TVN / CVE ID	TVN-202508003 / CVE-2025-9254
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	WebITR 2_1_0_32(含)以前版本
問題描述	凱發科技開發之WebITR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以任意使用者身分登入系統。
解決方法	更新至2_1_0_33(含)以後版本
公開日期	2025-08-20
相關連結	**https://www.twcert.org.tw/tw/cp-132-10328-dbc35-1.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8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/**