TWCERT/CC 資安情資電子報

2025 年 7 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

駭客偽冒通訊軟體，釣魚攻擊再升級

TWCERT/CC掌握外部威脅情資，駭客組織持續升級社交工程與釣魚攻擊手法，近期發現有駭客團體疑似偽冒通訊軟體，透過散布惡意程式或設置釣魚網站，引誘導使用者下載安裝，進而植入惡意程式，導致個人資料外洩或帳號盜用。

今(2025)年2月至3月間駭客組織偽冒知名通訊軟體，透過社交工程手法誘導使用者下載惡意檔案，進而植入惡意程式並竊取資料。依據調查顯示，已有多名使用者受害，相關攻擊活動影響範圍廣泛。

國家資通安全研究院分析惡意樣本後，發現駭客利用多層次封裝後門程式，配合社交工程與SEO偽冒網站的攻擊手法，致使防護機制與端點偵測工具不易辨識和阻擋。此惡意檔案除了包含基本後門模組、檔案管理模組、鍵盤側錄模組，還新增了遠端控制HVNC模組，可操控隱藏桌面。圖1為駭客組織使用SEO攻擊手法，圖2為駭客組織攻擊流程。

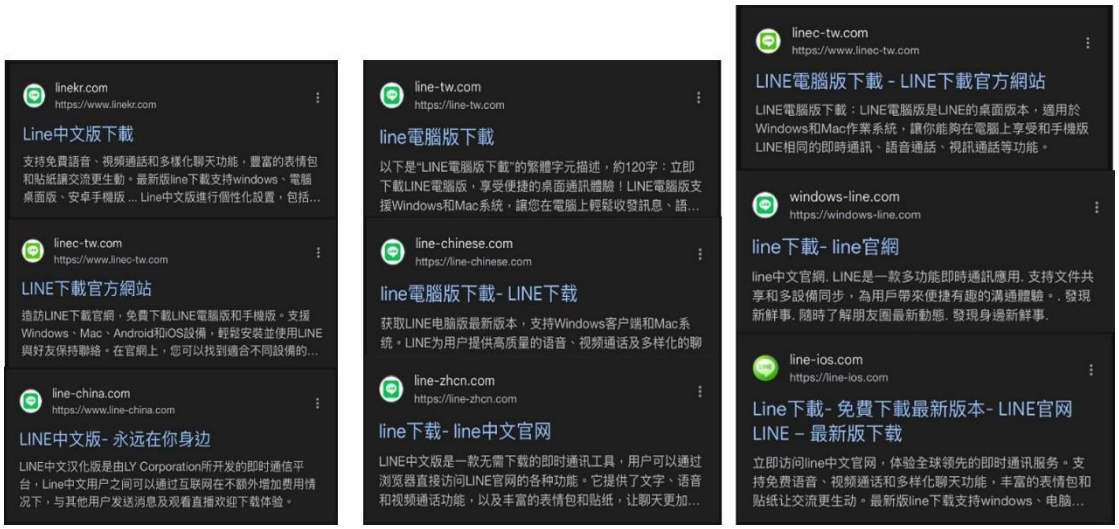

圖1：駭客組織使用SEO攻擊手法。圖片來源：資安院

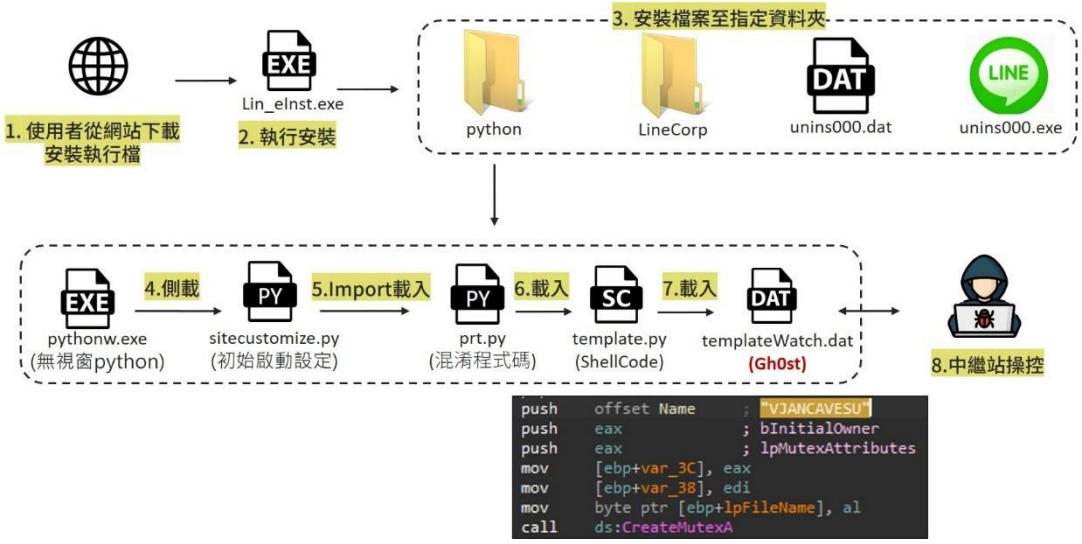

圖2：下載偽冒通訊軟體之攻擊流程圖。圖片來源：資安院

目前，2025年6月所使用的惡意檔案已能被主流防毒軟體偵測與攔

截，但資安監測發現，自7月起駭客持續推出變種版本，試圖繞過防護機制，顯示攻擊行動並未停止。建議使用者下載通訊軟體或任何應用程式時，務必前往官方網站或合法應用程式商店（如Google Play、Apple App Store）下載，切勿輕信來路不明的連結或第三方來源。此外，建議設備安裝可靠的防毒軟體，定期掃描系統，並保持軟體更新，以提升防護能力。對於可疑訊息或連結，應避免點擊或回應，若有疑慮，應主動向官方客服查證，確保資訊安全不受威脅。

以下是偽冒LINE網站之連結：

www[.]lineoe[.]com
www[.]linerm[.]com
www[.]linecl[.]com
www[.]line-tww[.]com

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 從Windows到Linux勒索軟體BERT的演化與擴散

BERT（又被趨勢科技稱作Water Pombero）於2025年4月首次被發現，是一種具備跨平台能力的勒索軟體，主要針對Windows和Linux環境發動攻擊。根據目前掌握的資訊，BERT勒索軟體的攻擊活動主要集中在亞洲與歐洲地區，受害對象則以醫療產業、科技公司以及事件管理服務等領域為主。

BERT最早針對Windows平台發起攻擊，透過PowerShell Loader（如start.ps1）取得初始存取，接著提升系統權限並停用 Windows Defender、防火牆及 UAC，再從遠端IP位址下載並執行勒索軟體，後續開始加密檔案，並加上「.encryptedbybert」副檔名，同時留下解密通知，如圖1所示。

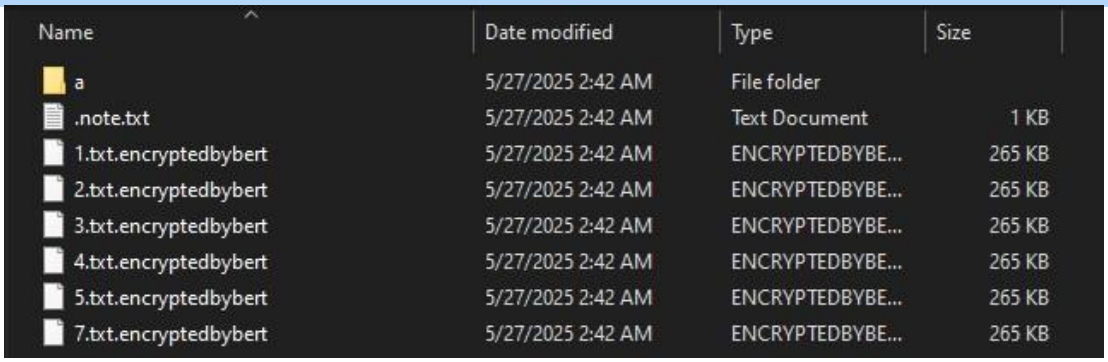

圖1：BERT勒索軟體在Windows的加密文件。圖片來源：TREND

近期，BERT勒索軟體進一步改良與精進，推出針對Linux系統的新變體。此版與知名勒索軟體Revil（Sodinokibi）在程式碼高達80%的相似度，顯示其技術來源與演進脈絡密切相關。BERT的技術特色包含可同時啟動50個CPU執行緒以提升加密效率，進而降低被偵測或中斷的風險，此外，還會強制關閉目標虛擬機的運作，以確保加密過程的完整性。完成加密後，所有檔案將被加上副檔名「.encrypted_by_bert」，如圖2所示。

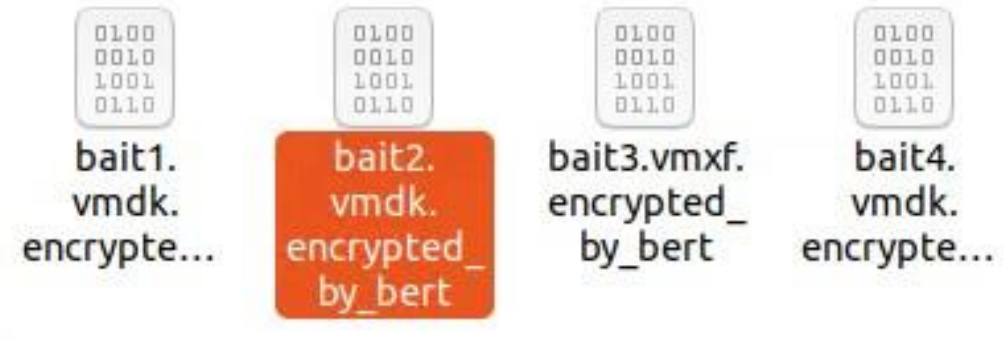

圖 2：BERT勒索軟體在Linux的加密文件。圖片來源：TREND

另外，BERT勒索軟體程式內部包含一組JSON配置檔，其中含公鑰(pk)、Base64 編碼的勒索信等詳細資料。這是現代勒索軟體常見的經典特徵，透過此方式，攻擊者可靈活針對不同場景進行調整與自訂。

為有效防範勒索軟體攻擊，建議可採取以下幾項關鍵措施：

1. 定期進行備份資料，並將備份儲存在與主要系統隔離的地方，如外部硬碟或雲端儲存空間。

2. 確保所有設備的作業系統與應用程式都保持在最新版本，藉此修補可能被駭客利用的安全漏洞。

3. 透過教育訓練提升使用者的安全意識，提升對可疑郵件和網路詐騙的辨識能力，有助於減少人為失誤所造成的風險。

4. 落實最小權原則，限制帳號權限以防止勒索軟體擴散至整個系統。

5. 組織或企業應部屬多層次的資安防護，例如防毒軟體、防火牆以及入侵偵測系統，以提高整體防禦能力。

6. 建立完整的資安事件應變計畫，並定期進行演練，有助在遭受攻擊時可快速反應，有效控管災損並儘速恢復正常運作。

以下是趨勢科技提供BERT勒索軟體的IoC：

1ef6c1a4dfdc39b63bfe650ca81ab89510de6c0d3d7c608ac5be80033e559326
70211a3f90376bbc61f49c22a63075d1d4ddd53f0aefa976216c46e6ba39a9f4
75fa5b506d095015046248cf6d2ec1c48111931b4584a040ceca57447e9b9d71
8478d5f5a33850457abc89a99718fc871b80a8fb0f5b509ac1102f441189a311
b2f601ca68551c0669631fd5427e6992926ce164f8b3a25ae969c7f6c6ce8e4f
bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4
c7efe9b84b8f48b71248d40143e759e6fc9c6b7177224eb69e0816cc2db393db
hxxp://185[.]100[.]157[.]74/payload[.]exe

- 相關連結
  1. BERT Ransomware Group Targets Asia and Europe on Multiple Platforms
  2. Bert Ransomware
  3. BERT Ransomware Can Force Shutdown of ESXi Virtual Machines to Hinder Recovery

2.2 新興應用資安

2.2.1 機密早已外洩！GitHub Actions 成內鬼溫床，寫入權限竟等同全權存取！

在開發流程自動化日益普及的時代，GitHub Actions 成為許多開發者不可或缺的工具。然而，資安研究人員提醒， GitHub Repository secrets 的設計存在潛在風險，只要擁有儲存庫寫入權限的使用者，就可能存取甚至竊取secrets。為了降低風險，建議使用 GitHub Environment secrets的保護規則和正確配置的 OIDC（OpenID Connect）信任策略，以強化憑證與密鑰的安全性。

除了機制設計問題外，初學者在撰寫GitHub Action Workflow 時的錯誤用法，也常造成機密洩漏風險。最常見的情況是直接將 secrets值寫入工作流程檔案中，使得敏感資訊如金鑰或密碼暴露於公開程式碼之中，嚴重威脅系統安全，如圖1所示。

```yaml
steps:
  - name: Checkout code
    uses: actions/checkout@v4

  - name: Configure AWS credentials
    uses: aws-actions/configure-aws-credentials@v4
    with:
      aws-access-key-id: AKIAIOSFODNN7EXAMPLE
      aws-secret-access-key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
      aws-region: us-east-1

  - name: Deploy Lambda
```

圖1：將secrets直接寫入Workflow上。圖片內容取自github: airman604

目前網路上廣為流傳的做法，是透過Github的介面在路徑「settings → secrets and variables → actions」中，設定Repository secrets，如圖2所示。設定完成後，開發者便可在GitHub Actions的Workflow中直接寫入變數的名稱，如圖3所示。這種方式表面上來看具備一定隱蔽性，因為UI 中無法直接查看密文內容，但實際上卻潛藏重大風險。

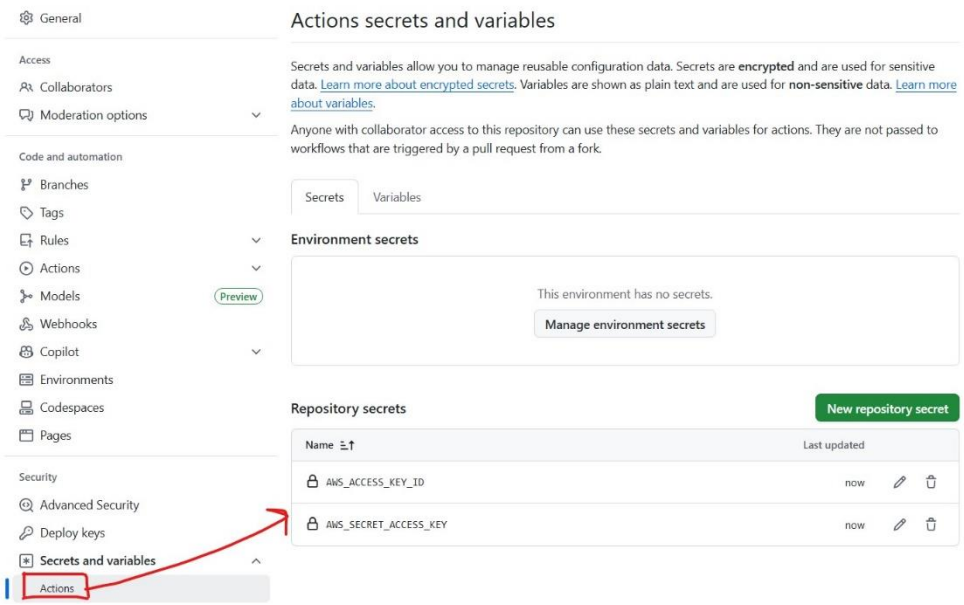

圖2：設定Repository secrets。TWCERT/CC整理

```
12          uses: actions/checkout@v4
13
14        - name: Configure AWS credentials
15          uses: aws-actions/configure-aws-credentials@v4
16          with:
17            aws-access-key-id: ${{ secrets.AWS_ACCESS_KEY_ID }}
18            aws-secret-access-key: ${{ secrets.AWS_SECRET_ACCESS_KEY }}
19            aws-region: us-east-1
20
21        - name: Deploy Lambda
```

圖3：在Workflow中設定 Repository secrets 。圖片內容取自 github: airman604

根據GitHub官方文件說明，如圖4所示，任何擁有儲存庫「寫入權限」的使用者，都能藉由修改 Workflow，間接「讀取」並外洩這些 secrets (機密資料)。因此，建議你確保在Workflow中使用的憑證權限要設為「最低必要權限」。若未妥善設定，攻擊者可建立自訂的Workflow，將secrets輸出到日誌或將其傳送至外部伺服器等手法，達到外洩目的，對組織資安造成實質威脅。圖5為使用者擁有寫入權限，即可輸出儲存在Workflow的機密資料。

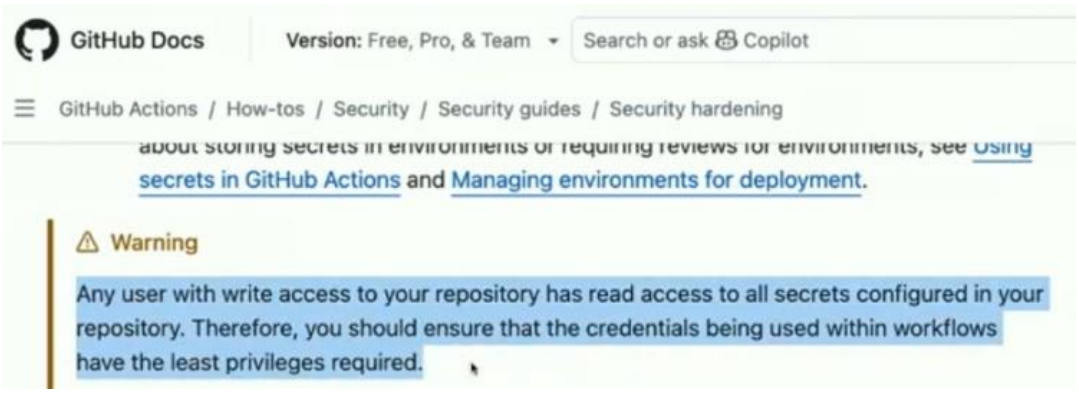

圖4: Github 官方說明。圖片內容取自 airman604

```yaml
jobs:
  deploy:
    runs-on: ubuntu-latest

    steps:
      - name: Checkout code
        uses: actions/checkout@v4

      - name: Deploy Lambda
        env:
          AWS_ACCESS_KEY_ID: ${{ secrets.AWS_ACCESS_KEY_ID }}
          AWS_SECRET_ACCESS_KEY: ${{ secrets.AWS_SECRET_ACCESS_KEY }}
        run: |
          echo ">>>>>>>>  Validate GitHub Actions masking <<<<<<<<"
          echo "$AWS_ACCESS_KEY_ID"
          echo "$AWS_SECRET_ACCESS_KEY"
          echo ">>>>>>>>  NOM NOM NOM <<<<<<<<"
          echo "$AWS_ACCESS_KEY_ID" | base64
          echo "$AWS_SECRET_ACCESS_KEY" | base64
```

圖5: 示範列印Secrets。圖片內容取自 github: airman604

為了因應上述風險，推薦使用Github的Environment secrets搭配部署保護規則（deployment protection rules）。這項機制允許開發者在每個環境設定獨立的secrets，並透過細緻的保護規則控管其使用條件。當Workflow中的某個job嘗試存取指定環境的secrets時，必須先通過該環境設定的保護規則，才能取得執行權限。設定的路徑為「settings→ secrets and variables→ actions」，如圖 6 所示。

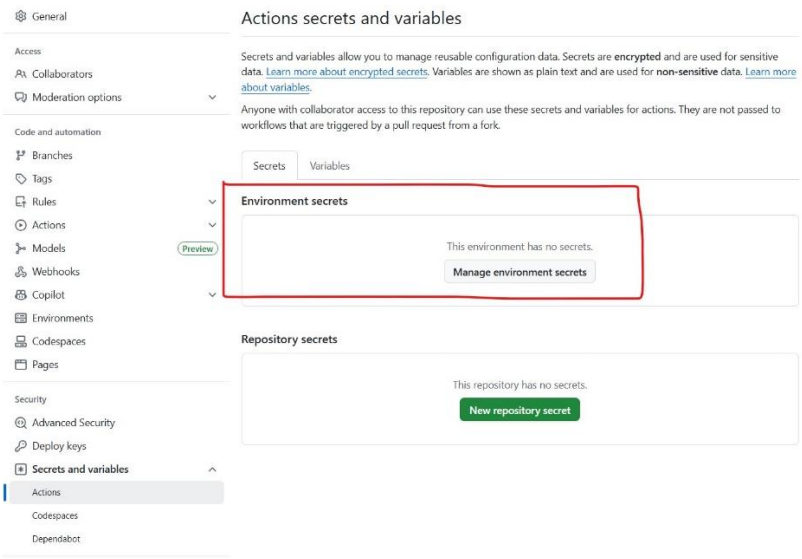

圖6: 設定 Environment secrets 位置。TWCERT/CC整理

另一項有效強化措施是利用OIDC（OpenID Connect）結合AWS IAM，以避免在 GitHub 儲存庫中長期儲存敏感憑證。當使用者有請求時，透過Github Action 動態請求AWS所提供的短期憑證，即使工作流程被竄改，也只有在允許的條件下才取得憑證。

以下是Environment Secrets和OIDC + IAM Role二種方式比較表：

項目	Environment Secrets	OIDC + IAM Role
憑證型態	長期憑證	短期憑證（每次執行產生）
存取控制細緻度	中等（只能限制環境）	高（可限制分支、環境、儲存庫、觸發者）
風險	一旦洩漏可長期使用	洩漏後短期失效
可審核性	有一定限制	高，可搭配 AWS CloudTrail、IAM 認證紀錄
複雜度	簡單	稍高，需要 AWS IAM 與信任策略設定

- 相關連結
  1. Not So Secret: The Hidden Risks of GitHub Actions Secrets

2.3 軟體系統資安議題

2.3.1 CitrixBleed2漏洞可能引發記憶體資料外洩風險

近期Citrix發布二項嚴重資安漏洞公告，分別為CVE-2025-5777（CVSS 4.x：9.3）與CVE-2025-6543（CVSS 4.x：9.2），並已釋出修補程式以應對攻擊威脅，這二個漏洞主要影響Citrix NetScaler ADC 與Gateway設備，特別是版本13.1及14.1以下。此外，部分受影響的NetScaler版本已達生命週期終止（EoL），建議用戶儘速升級至支援版本以確保安全，因漏洞涉及記憶體溢位與記憶體越界，攻擊者可能藉此取得系統記憶體中的敏感資料，如使用者登入憑證、有效的Session Token以及記憶體中處理的HTTP請求內容等，攻擊者可能繞過多因子驗證機制，造成嚴重的資料外洩風險。

美國網路安全暨基礎設施安全局（CISA）已於7月10日和6月30日將這二個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，並加強監控異常存取行為。研究人員建議除了立即套用官方修補程式外，還應註銷現有Citrix Session Token、更換登入密碼，並部署Web應用防火牆（WAF）以阻擋未經授權的請求，降低被攻擊風險。

CVE-2025-5777 漏洞源於Citrix處理登入請求的「/p/u/doAuthentication.do」端點使用錯誤snprintf寫法，導致login欄位未進行正確的初始化，造成記憶體溢位並回傳堆疊中殘留資料，進而引發資料洩漏。由於格式字串為「%.*s」，因此每次洩漏的資料皆不同，攻擊者若持續嘗試多次並拼湊這些記憶體內容，便能逐步還原更多敏感資訊，如圖1所示。

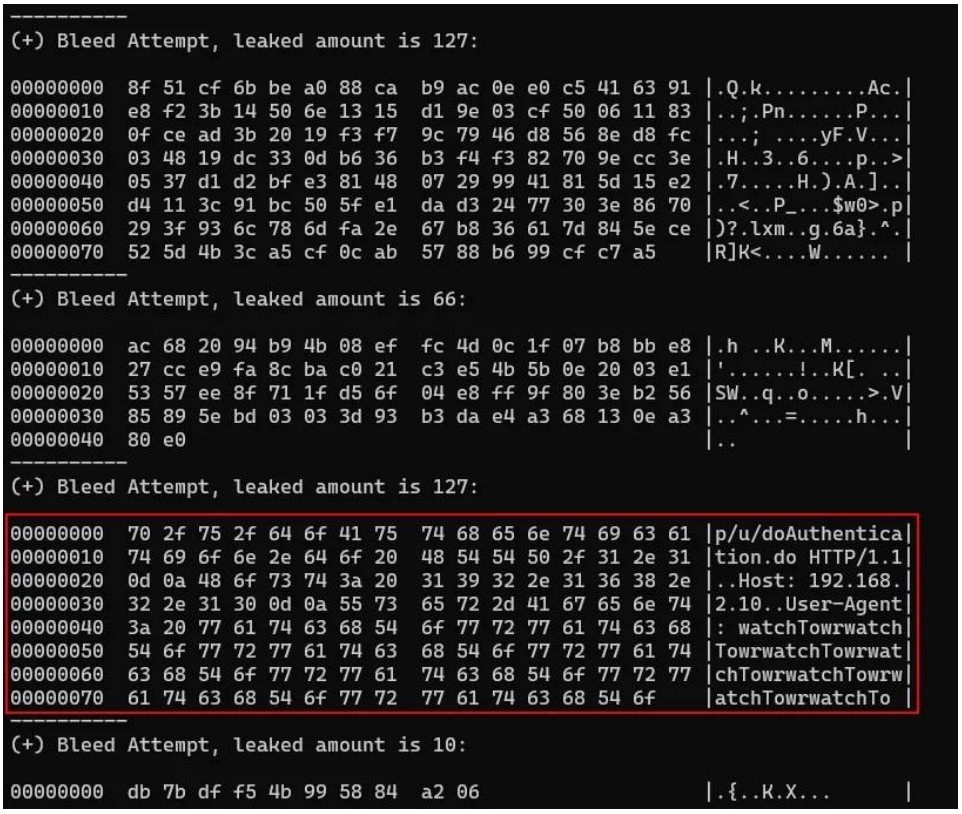

圖1：Labs研究人員針對CVE-2025-5777之實驗結果。圖片來源：Labs

值得注意的是，CVE-2025-5777被稱為「CitrixBleed 2」，與2023年爆發的CitrixBleed漏洞（CVE-2023-4966，CVSS 3.x：9.4）類似，該漏洞曾被勒索團體利用，且已有公開可利用程式碼，意味著可能攻擊已在進行中，企業必須迅速行動以防止資安事件擴大，以下是根據這次漏洞公告的建議和防護措施：

1. 強制登出所有現有的Session，避免被舊憑證劫持
2. 盤點現有使用的Citrix設備版本與配置，確認是否受影響
3. 持續關注廠商公告，確保組織可在第一時間進行更新
4. 部署入侵防禦系統（IDS/IPS）及Web應用防火牆（WAF），攔截異常請求
5. 加強內部監控與異常行為分析，及早發現攻擊跡象

由於PoC已公開且漏洞已被證實積極利用，企業必須儘速採取更新行動。此外，資安防護的第一步是清楚掌握企業內部所有設備的狀態與版本，並持續追蹤廠商的安全更新與公告，必免因疏忽而成為攻擊目標。

- 相關連結

1. CISA Adds Citrix NetScaler CVE-2025-5777 to KEV Catalog as Active Exploits Target Enterprises
2. CISA Adds Four Critical Vulnerabilities to KEV Catalog Due to Active Exploitation
3. Public exploits released for Citrix Bleed 2 NetScaler flaw, patch now
4. CVE-2025-5777: CitrixBleed 2 Write-Up… Maybe?
5. CitrixBleed 2 exploitation started mid-June — how to spot it
6. How Much More Must We Bleed? - Citrix NetScaler Memory Disclosure (CitrixBleed 2 CVE-2025-5777)

2.4 軟硬體漏洞資訊

2.4.1 Cisco旗下Unified Communications Manager存在重大資安漏洞

CVE 編號	CVE-2025-20309
影響產品	Cisco Unified Communications Manager
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-cucm-ssh-m4UBdpE7

- 內容說明：

  Cisco Unified Communications Manager（Unified CM）和 Cisco Unified Communications Manager Edition（Unified CM SME）是 Cisco 提供的統一通訊平台，主要支援語音、視訊、訊息和協同作業功能。日前，Cisco 發布重大資安漏洞公告(CVE-2025-20309，CVSS：10.0)，該漏洞源於產品中內建的預設靜態憑證，其所對應的 root 帳戶為預設存在，且無法由使用者修改或刪除。此漏洞可能允許未經身分驗證的遠端攻擊者，以 root 權限登入受影響設備並執行任意指令。

- 影響平台：
  - Cisco Unified Communications Manager 15.0.1.13010-1 至 15.0.1.13017-1 版本

- 資料來源：
  1. Cisco Unified Communications Manager Static SSH Credentials Vulnerability
  2. CVE-2025-20309

2.4.2 Fortinet旗下FortiWeb存在重大資安漏洞

CVE 編號	CVE-2025-25257
影響產品	FortiWeb
解決辦法	請更新至 FortiWeb 7.0.11 版本、FortiWeb 7.2.11 版本、FortiWeb 7.4.8 版本、FortiWeb 7.6.4 版本

- 內容說明：

  Fortinet 旗下 FortiWeb 是一款提供網站應用程式的防火牆產品，其功能涵蓋異常偵測、API 保護、機器人緩解和進階威脅分析等。日前，Fortinet 發布重大資安漏洞公告(CVE-2025-25257，CVSS：9.6)，此漏洞可能允許未經身分驗證的攻擊者，透過精心設計的 HTTP 或 HTTPs 請求未經授權的 SQL 程式碼或命令。

- 影響平台：
  - FortiWeb 7.0.0 至 7.0.10 版本
  - FortiWeb 7.2.0 至 7.2.10 版本
  - FortiWeb 7.4.0 至 7.4.7 版本
  - FortiWeb 7.6.0 至 7.6.3 版本
- 資料來源：
  1. Unauthenticated SQL injection in GUI
  2. CVE-2025-25257

2.4.3 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2025-42967,CVE-2025-42980,CVE-2025-42964,CVE-2025-42966,CVE-2025-42963
影響產品	SAP S/4HANA、SCM Characteristic Propagation、NetWeaver Enterprise Portal Federated Portal Network、NetWeaver Enterprise Portal Administration、NetWeaver XML Data Archiving、NetWeaver Application server
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/july-2025.html

- 內容說明：

  【CVE-2025-42967，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程式碼建立文件，可能完全控制受影響的 SAP 系統。

  【CVE-2025-42980，CVSS：9.1】

  該漏洞存在於 SAP NetWeaver Enterprise Portal Federated Portal Network，允許特權使用者上傳不受信任或惡意內容，這些內容反序列化後可能導致主機系統受損害。

  【CVE-2025-42964，CVSS：9.1】

  該漏洞存在於 SAP NetWeaver Enterprise Portal Administration，允許特權使用者上傳不受信任或惡意內容，這些內容反序列化後可能導致主機系統受損害。

  【CVE-2025-42966，CVSS：9.1】

SAP NetWeaver XML Data Archiving 服務存在 Java 反序列化漏洞，允許經過驗證且擁有管理者權限的攻擊者，利用精心設計的序列化 Java 物件影響應用程式的機密性、完整性及可用性。

【CVE-2025-42963，CVSS：9.1】

SAP NetWeaver Application server 的 Java Log 存在 Java 反序列化漏洞，允許經過驗證且擁有管理者權限的攻擊者，可完全控制受影響的系統，嚴重影響應用程式和主機環境的機密性、完整性及可用性。

- 影響平台：
  - SCMAPO 713,714
  - S4CORE 102,103,104
  - S4COREOP 105,106,107,108
  - SCM 700,701,702,712
  - EP-RUNTIME 7.50
  - J2EE-APPS 7.50
  - LMNWABASICAPPS 7.50
- 資料來源：
  1. SAP Security Patch Day - July 2025
  2. CVE-2025-42967
  3. CVE-2025-42980
  4. CVE-2025-42964
  5. CVE-2025-42966
  6. CVE-2025-42963

2.4.4 VMware ESXi、Workstation、Fusion 和 Tools 存在3個重大資安漏洞

CVE 編號	CVE-2025-41236,CVE-2025-41237,CVE-2025-41238
影響產品	VMware ESXi、Workstation、Fusion
解決辦法	根據官方網站釋出的解決方式進行修補： https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877

- 內容說明：

  【CVE-2025-41236，CVSS：9.3】

  VMware ESXi、Workstation 和 Fusion 的 VMXNET3 虛擬網路介面卡存在整數溢位漏洞。

  【CVE-2025-41237，CVSS：9.3】

  VMware ESXi、 Workstation 和 Fusion 的 VMCI 存在整數下溢漏洞，可能導致越界寫入。

  【CVE-2025-41238，CVSS：9.3】

  VMware ESXi、Workstation 和 Fusion 的 PVSCSI 控制器存在堆疊溢位漏洞，可能導致越界寫入。

- 影響平台：
  - VMware Cloud Foundation
  - VMware vSphere Foundation
  - VMware ESXi
  - VMware Workstation Pro
  - VMware Fusion
  - VMware Tools
  - VMware Telco Cloud Platform
  - VMware Telco Cloud Infrastructure
- 資料來源：

1. VMSA-2025-0013: VMware ESXi, Workstation, Fusion, and Tools updates address multiple vulnerabilities
2. CVE-2025-41236
3. CVE-2025-41237
4. CVE-2025-41238

2.4.5 Cisco 旗下身分識別服務存在重大資安漏洞

CVE 編號	CVE-2025-20337
影響產品	Cisco ISE、ISE-PIC
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-ise-unauth-rce-ZAd2GnJ6

- 內容說明：

  Cisco 旗下身分識別服務引擎(Identity Services Engine，ISE)是一款基於身分的安全管理平台，可從網路、使用者設備收集資訊，並在網路基礎設施中實施策略和制定監管決策。Cisco 發布重大資安漏洞公告(CVE-2025-20337，CVSS：10.0)並釋出更新版本，此漏洞存在於 Cisco ISE 和 Cisco ISE-PIC 的特定 API，攻擊者無需任何有效憑證即可利用此漏洞，允許未經身分驗證的遠端攻擊者以 root 身分在底層作業系統上執行任意程式碼。

- 影響平台：
  - Cisco ISE 和 ISE-PIC 3.3、3.4 版本
- 資料來源：
  1. Cisco Identity Services Engine Unauthenticated Remote Code Execution Vulnerabilities
  2. CVE-2025-20337

2.4.6 WordPress近期公布10個擴充功能相關安全漏洞，請儘速確認並進行修補

CVE 編號	CVE-2020-36847,CVE-2020-36849,CVE-2025-5392,CVE-2025-5393,CVE-2025-5394,CVE-2025-6058,CVE-2025-7340,CVE-2025-7341,CVE-2025-7360,CVE-2025-7401
影響產品	WordPress Simple-File-List、AIT CSV import/export、Plugin-GB Forms DB、Alone – Charity Multipurpose Non-profit、WPBookit、HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder、Premium Age Verification / Restriction
解決辦法	更新 AIT CSV import/export 至 3.0.4(含)以前版本 更新 Alone – Charity Multipurpose Non-profit 至 7.8.5(含)以後版本 更新 GB Forms DB 至 1.0.3(含)以後版本 更新 HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder 至 2.2.2(含)以後版本 Premium Age Verification / Restriction 尚未釋出修補程式，建議先停用該功能 更新 Simple-File-List 至 4.2.3(含)以後版本 更新 WPBookit 至 1.0.5(含)以後版本

- 內容說明：

  CVE-2020-36847：

  WordPress 之擴充程式 Simple-File-List，未妥善限制命名功能之使用，允許未經身分鑑別之遠端攻擊者上傳合法檔名之網頁後門程式後，透過修改檔名使其可於伺服器上執行。

  CVE-2020-36849：

WordPress 之擴充程式 AIT CSV import/export 未妥善驗證上傳檔案，允許未經身分鑑別之遠端攻擊者上傳網頁後門程式並於伺服器上執行。

CVE-2025-5392：

WordPress 之擴充程式 Plugin-GB Forms DB 未妥善過濾使用者輸入，允許未經身分鑑別之遠端攻擊者注入程式碼並於伺服器上執行。

CVE-2025-5393：

WordPress 之網頁主題 Alone – Charity Multipurpose Non-profit 未妥善驗證檔案路徑參數，允許未經身分鑑別之遠端攻擊者刪除任意伺服器檔案。

CVE-2025-5394：

WordPress 之網頁主題 Alone – Charity Multipurpose Non-profit 未妥善驗證上傳檔案，允許未經身分鑑別之遠端攻擊者上傳網頁後門程式並於伺服器上執行。

CVE-2025-6058：

WordPress 之擴充程式 WPBookit 未妥善驗證上傳檔案，允許未經身分鑑別之遠端攻擊者上傳網頁後門程式並於伺服器上執行。

CVE-2025-7340：

WordPress 之擴充程式 HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder 未妥善驗證上傳檔案，允許未經身分鑑別之遠端攻擊者上傳網頁後門程式並於伺服器上執行。

CVE-2025-7341：

WordPress 之擴充程式 HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder 未妥善驗證檔案路徑參數，允許未經身分鑑別之遠端攻擊者刪除任意伺服器檔案。

CVE-2025-7360：

WordPress 之擴充程式 HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder 未妥善驗證檔案路徑參數，允許未經身分鑑別之遠端攻擊於伺服器上移動任意檔案至任意路徑。

CVE-2025-7401：

WordPress 之擴充程式 Premium Age Verification / Restriction，為妥善保護特定功能，允許未經身分鑑別之遠端攻擊者讀取與寫入任意伺服器檔案。

以上漏洞皆有遠端程式碼執行之風險，請儘速確認並進行修補。

- 影響平台：
  - AIT CSV import/export 3.0.3(含)以前版本
  - Alone – Charity Multipurpose Non-profit 7.8.3(含)以前版本
  - GB Forms DB 1.0.2(含)以前版本
  - HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder 2.2.1(含)以前版本
  - Premium Age Verification / Restriction 3.0.2(含)以前版本
  - Simple-File-List 4.2.2(含)以前版本
  - WPBookit 1.0.4(含)以前版本
- 資料來源：
  1. https://nvd.nist.gov/vuln/detail/CVE-2020-36847
  2. https://nvd.nist.gov/vuln/detail/CVE-2020-36849
  3. https://nvd.nist.gov/vuln/detail/CVE-2025-5392
  4. https://nvd.nist.gov/vuln/detail/CVE-2025-5393
  5. https://nvd.nist.gov/vuln/detail/CVE-2025-5394
  6. https://nvd.nist.gov/vuln/detail/CVE-2025-6058
  7. https://nvd.nist.gov/vuln/detail/CVE-2025-7340
  8. https://nvd.nist.gov/vuln/detail/CVE-2025-7341
  9. https://nvd.nist.gov/vuln/detail/CVE-2025-7360
  10. https://nvd.nist.gov/vuln/detail/CVE-2025-7401
  11. https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ait-csv-import-export/ait-c

2.4.7 Sophos 旗下Intercept X for Windows 存在2個重大資安漏洞

CVE 編號	CVE-2024-13972,CVE-2025-7433
影響產品	Sophos Intercept X for Windows
解決辦法	根據官方網站釋出解決方式進行修補： https://www.sophos.com/en-us/security-advisories/sophos-sa-20250717-cix-lpe

- 內容說明：

  【CVE-2024-13972，CVSS：8.8】

  此漏洞存在於 Sophos Intercept X for Windows 的更新程式中，與登錄檔權限設定有關。攻擊者可能在產品升級期間，透過本機使用者取得系統層級的權限。

  【CVE-2025-7433，CVSS：8.8】

  在 Sophos Intercept X for Windows 的裝置加密元件中存在本機權限提升漏洞，此漏洞允許攻擊者執行任意程式碼。

- 影響平台：
  - Sophos Intercept X for Windows 2024.3.2 (不含)以前版本
  - Sophos Intercept X for Windows Central Device Encryption 2025.1 (不含)以前版本
- 資料來源：
  1. Resolved Multiple Vulnerabilities in Sophos Intercept X for Windows
  2. CVE-2024-13972
  3. CVE-2025-7433

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

CVE 編號	CVE-2025-49704,CVE-2025-53770
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： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770

- 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。

  【CVE-2025-49704，CVSS：8.8】

  此為程式碼注入漏洞，允許經過授權的攻擊者遠端執行任意程式碼。

  【CVE-2025-53770，CVSS：9.8】

  此為不受信任資料之反序列化漏洞，允許未經授權的攻擊者執行任意程式碼。

  此外，據目前情資，發現 Microsoft SharePoint 的 CVE-2025-49704、CVE-2025-49706 及 CVE-2025-53770 已遭駭客利用，請儘速完成更新作業，並檢視是否有遭異常存取情況。

- 影響平台：
  - Microsoft SharePoint Enterprise Server 2016
  - Microsoft SharePoint Server 2019
  - Microsoft SharePoint Enterprise Server 2016
  - Microsoft SharePoint Server 2019
  - Microsoft SharePoint Server Subion Edition
- 資料來源：
  1. Microsoft SharePoint Remote Code Execution Vulnerability

2. Microsoft SharePoint Server Remote Code Execution Vulnerability
3. CVE-2025-49704
4. CVE-2025-53770

2.4.9 Sophos 的防火牆系統存在3個重大資安漏洞

CVE 編號	CVE-2025-6704,CVE-2025-7624,CVE-2025-7382
影響產品	Sophos Firewall
解決辦法	根據官方網站釋出解決方式進行修補： https://www.sophos.com/en-us/security-advisories/sophos-sa-20250721-sfos-rce

- 內容說明：

  Sophos 發布關於防火牆的資安公告，指出旗下的防火牆產品存在 3 個重大資安漏洞，並提出修補版本，呼籲用戶儘快檢查系統是否套用相關更新。

  【CVE-2025-6704，CVSS：9.8】

  安全 PDF 交換(Secure PDF eXchange，SPX)功能存在任意文件寫入漏洞，若啟用 SPX 的特定配置且防火牆處於高可用性(HA)模式，可能導致預授權遠端程式碼執行。

  【CVE-2025-7624，CVSS：9.8】

  Legacy (transparent) SMTP proxy 存在一項 SQL 注入漏洞，若電子郵件啟用隔離政策，且系統從 21.0 GA 之前的版本升級至現有版本，可能導致遠端程式碼執行。

  【CVE-2025-7382，CVSS：8.8】

  WebAdmin 存在命令注入漏洞，若管理員啟用 OTP 驗證，則可能導致相鄰攻擊者在高可用性(HA)輔助設備上實現預授權程式碼執行。

  TMEE 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的 TMEE 安裝執行任意程式碼。

- 影響平台：
  - Sophos Firewall v21.5 GA (含)以前版本

- 資料來源：
  1. Resolved Multiple Vulnerabilities in Sophos Firewall
  2. CVE-2025-6704
  3. CVE-2025-7624
  4. CVE-2025-7382

2.4.10 SonicWall 旗下SMA100系列產品存在重大資安漏洞

CVE 編號	CVE-2025-40599
影響產品	SonicWall SMA100
解決辦法	更新 SMA 100 系列產品至 10.2.2.1-90sv (含)之後版本

- 內容說明：

  SonicWall 針對 SMA100 系列產品發布重大資安漏洞(CVE-2025-40599，CVSS：9.1)，SMA100 系列產品的 Web 管理介面存在經過驗證的任意檔案上傳漏洞，遠端攻擊者若具有管理員權限，便可藉此上傳任意檔案至系統，可能導致遠端程式碼執行。

- 影響平台：
  - SMA 100 系列產品 10.2.1.15-81sv(含)之前版本
- 資料來源：
  1. SonicWall SMA100 Post-authentication Arbitrary File Upload vulnerability
  2. CVE-2025-40599

第 3 章、資安研討會及活動

- **資安研討會**

【數位產業署】8/8資服業者個資交流工作坊(經營醫療系統資服業者為優先)	
活動時間	**2025/08/08(五) 13:00 ~ 16:20**
活動地點	**DigiBlock C數位創新基地(臺北市大同區承德路三段287號C棟)**
活動網站	**https://www.cisanet.org.tw/Course/Detail/5751**
活動概要	 **【費用】** 免費 報名截止： 2025/08/07 **【課程目標 / Event Deails】** 面對個資法，別再單打獨鬥！本場交流工作坊邀請法律與個資專家現身說法，帶您快速掌握個資法法遵要點、撰寫「個資安全維護計畫」實務技巧，並透過分組討論，讓您與專家面對面交流，針對企

	業在實務運用上的疑難雜症，獲得具體建議與解方。 **【主辦單位】數位部數位產業署** **【執行單位】財團法人資訊工業策進會、中華民國資訊軟體協會** **【聯絡窗口】02-2553-3988 分機 816 林專員** **security@cisanet.org.tw**
【資安學院】8/12 全面掌握VMS弱點管理系統及修補技巧一從識別到修補，提升企業安全防護的實用課程	
活動時間	**2025-08-12 13:30 ~ 17:30**
活動地點	**中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/5426**
活動概要	 **【費用】** 原價：4,800元/人 早鳥價：4,500元/人 軟協會員：4,000元/人 費用含稅、教材及完課證明 報名截止： 2025-08-07 **【課程內容 / Event Deails】** 為保障資訊資產安全，定期執行弱點掃描或滲透測試是必要的檢測工作。其中，弱點掃描主要用以找出已知、已公開的作業系統、應

	用程式或設備韌體上的漏洞。然而，在產出弱點掃描報告後，面對一長串的資料又該如何下手？ 本課程將教導學員弱點修補邏輯判斷原則、常見弱點類型、針對各類弱點劃分風險等級並提出改善建議。讓您得以優先處理衝擊最大之弱點、有效地控制風險，進而強化企業資安韌性。 **【主辦單位】中華民國資訊軟體協會** **【聯絡窗口】02-2553-3988 分機 816 林專員** **security@cisanet.org.tw**
【資安學院】8/13 駭客入侵防護實務	
活動時間	**2025/8/13 09:00 - 16:00**
活動地點	**中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/5441**
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： 2025/08/06 **【活動內容 / Event Deails】**

	隨著數位時代的來臨，網路安全議題儼然已成為當代人們不得不關注的問題。網站安全的實用指南，提供全面且易於操作的解決方案。從基礎到進階層面，涵蓋各種網站所需的知識和技巧。本課程內容先介紹基本安全措施，接著透過實務攻擊 DEMO 操作，讓您了解各種入侵思路，如：控制訪問權限、常見網站安全入侵手法等。再進一步強化系統安全，探討安全配置與即時安全監測。以深入淺出的方式，使學員在短時間內掌握駭客入侵防護的重要概念，並能藉此對網路安全有更深刻的理解，且能應用所學。 **【主辦單位】中華民國資訊軟體協會** **【聯絡窗口】02-2553-3988 分機 816 林專員** **security@cisanet.org.tw**
【資安學院】8/28-8/29 滲透測試與應用實務(實作課)	
活動時間	**2025-08-28 09:00 ~ 2025-08-28 17:00**
活動地點	**中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/5442**
活動概要	 **【費用】** 原價：12,000元/人 早鳥價：11,000元/人 軟協會員：9,500元/人 費用含稅、教材、餐點及完課證明

	報名截止： 2025-08-22 **【課程內容 / Event Deails】** 應用系統與軟體的漏洞是駭客強大的武器。因此，軟體開發、管理人員除熟悉安全軟體開發方法外，更需了解駭客攻擊原理與步驟，並透過模擬真實攻擊行為，方能知曉採取何者應對措施。本課程將說明駭客可能之攻擊手法，輔以實例，教導您資訊蒐集、漏洞挖掘進而遠端操控之方法，以及如何建立及操作持久性後門，讓您學習有效的資安防禦實務。 **【主辦單位】中華民國資訊軟體協會** **【聯絡窗口】02-2553-3988 分機 816 林專員** **security@cisanet.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：

桓基科技｜iSherlock - OS Command Injection	
TVN / CVE ID	TVN-202507003 / CVE-2025-7451
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	影響產品與版本： Hgiga iSherlock (包含 MailSherlock、SpamSherlock、AuditSherlock)4.5、5.5 影響套件： iSherlock-maillog-4.5 < 137 iSherlock-smtp-4.5 < 732 iSherlock-maillog-5.5 < 137 iSherlock-smtp-5.5 < 732
問題描述	桓基科技開發之iSherlock存在OS Command Injection漏洞，允許未經身分鑑別之遠端攻擊者注入任意作業系統指令並於伺服器上執行。此漏洞已遭開採利用，請盡速更新。
解決方法	更新套件iSherlock-maillog-4.5至137(含)以後版本 更新套件iSherlock-smtp-4.5至732(含)以後版本 更新套件iSherlock-maillog-5.5至137(含)以後版本 更新套件iSherlock-smtp-5.5至732(含)以後版本
公開日期	2025-07-11
相關連結	https://www.twcert.org.tw/tw/cp-132-10237-9e0f7-1.html
葳橋資訊｜簽章服務(BatchSignCS) - Arbitrary File Write through Path	

Traversal	
TVN / CVE ID	TVN-202507004 / CVE-2025-7619
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
影響產品	簽章服務(BatchSignCS) 3.138(含)以前版本
問題描述	葳橋資訊開發之簽章服務(BatchSignCS)為Windows背景程式，其存在Arbitrary File Write漏洞，在該程式開啟的情況下，使用者若瀏覽惡意網站，遠端攻擊者便可寫入任意檔案至任意路徑，並有機會利用此漏洞執行任意程式碼。
解決方法	更新至3.145(含)以後版本
公開日期	2025-07-14
相關連結	**https://www.twcert.org.tw/tw/cp-132-10239-770ab-1.html**
帝緯系統整合｜公文製作跨瀏覽器元件 - Remote Code Execution	
TVN / CVE ID	TVN-202507005 / CVE-2025-7620
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
影響產品	公文製作跨瀏覽器元件v1.6.8(含)以前版本
問題描述	帝緯系統整合製作之公文製作跨瀏覽器元件存在 Remote Code Execution漏洞，若使用者在該元件啟用的情況下瀏覽惡意網站，遠端攻擊者可使其下載任意程式並執行。
解決方法	聯繫廠商進行更新
公開日期	2025-07-14
相關連結	**https://www.twcert.org.tw/tw/cp-132-10241-2ec07-1.html**
達煬科技｜WinMatrix3 - Insecure Deserialization	
TVN / CVE ID	TVN-202507007 / CVE-2025-7916

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	WinMatrix AP 3.8.52.5(含)以前版本
問題描述	達煬科技開發之WinMatrix3應用程式伺服器端存在Insecure Deserialization漏洞，未經身分鑑別之遠端攻擊者可以透過發送惡意序列化內容於伺服器端執行任意程式碼。
解決方法	更新AP至3.8.52.5(Web 1.2.39.5)並安裝hotfix， 或更新AP至3.9.1(Web 1.3.1)(含)以後版本
公開日期	2025-07-21
相關連結	**https://www.twcert.org.tw/tw/cp-132-10256-14d55-1.html**
達煬科技｜WinMatrix3 Web套件 - SQL Injection	
TVN / CVE ID	TVN-202507009 / CVE-2025-7918
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	WinMatrix Web 1.2.39.5(含)以前版本
問題描述	達煬科技開發之WinMatrix3 Web套件存在SQL Injection漏洞，未經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	更新AP至3.8.52.5(Web 1.2.39.5)並安裝hotfix，或更新AP至3.9.1(Web 1.3.1)(含)以後版本
公開日期	2025-07-21
相關連結	**https://www.twcert.org.tw/tw/cp-132-10259-b4b38-1.html**
亞旭｜數據機 - Stack-based Buffer Overflow	
TVN / CVE ID	TVN-202507012 / CVE-2025-7921
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	設備型號：RTF8207w與RTF8217 韌體版本：R82XXR250718(不含)以前版本
問題描述	亞旭開發之部分數據機型號存在Stack-based Buffer Overflow漏洞，未經身分鑑別之遠端攻擊者可控制程式執行流程，並有機會執行任意程式碼。
解決方法	更新韌體版本至R82XXR250718(含)以後版本
公開日期	2025-07-21
相關連結	**https://www.twcert.org.tw/tw/cp-132-10268-1583b-1.html**
鼎新數智｜SFT - SQL Injection	
TVN / CVE ID	TVN-202507013 / CVE-2025-7343
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	SFT 3.7.12(含)以下版本
問題描述	鼎新數智開發之SFT存在SQL Injection漏洞，未經身分鑑別之遠端攻擊者可注入任意SQL指令以存取、修改或刪除資料庫內容。
解決方法	更新至3.7.4.5(含)以上版本並安裝修補程式KB202505001
公開日期	2025-07-21
相關連結	**https://www.twcert.org.tw/tw/cp-132-10270-83d95-1.html**
鼎新數智｜互聯中台 - Privilege Escalation	
TVN / CVE ID	TVN-202507014 / CVE-2025-7344
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	互聯中台 2.5.1 build 0161(含)以下版本

問題描述	鼎新數智開發之互聯中台存在Privilege Escalation漏洞，已經取得一般權限之遠端攻擊者可利用特定API取得管理員權限。
解決方法	更新至2.3.2 build 0115(含)以上版本並安裝修補程式KB202504001
公開日期	2025-07-21
相關連結	https://www.twcert.org.tw/tw/cp-132-10272-5b691-1.html
飛宇高新科技｜多功能智慧校園平台 - Missing Authorization	
TVN / CVE ID	TVN-202507015 / CVE-2025-8322
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	多功能智慧校園平台
問題描述	飛宇高新科技多功能校園平台存在Missing Authorization漏洞，已取得一般使用者權限之遠端攻擊者能夠直接存取管理員功能，包括新增、修改與刪除帳號，甚至可將任意帳號提升為系統管理員。
解決方法	系統執行於地端之學校單位，請聯繫飛宇高新科技確認單位更新狀況；或評估關閉對外服務、僅開放校內使用。
公開日期	2025-07-30
相關連結	https://www.twcert.org.tw/tw/cp-132-10304-6b375-1.html
飛宇高新科技｜多功能智慧校園平台 - Arbitrary File Upload	
TVN / CVE ID	TVN-202507016 / CVE-2025-8323
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	多功能智慧校園平台
問題描述	飛宇高新科技多功能校園平台存在Arbitrary File Upload漏

	洞，已取得一般使用者權限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	系統執行於地端之學校單位，請聯繫飛宇高新科技確認單位更新狀況；或評估關閉對外服務、僅開放校內使用。
公開日期	2025-07-30
相關連結	**https://www.twcert.org.tw/tw/cp-132-10306-ccea7-1.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7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/**