# TWCERT/CC 資安情資電子報

## 2025 年 3 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

## 防範社交工程！駭客利用網站假冒手法進行攻擊


TWCERT/CC近期接獲外部情資，駭客社交工程手法更為精細，為取信於收件者，將依據收件者輸入公司域名，動態產生相應的登入頁面，進一步提高網站的可信度。建議企業與使用者加強社交工程防護措施。

情資顯示，攻擊者寄送包含釣魚連結於附檔之惡意電子郵件，當收件人開啟附件並點擊連結後，會被引導至釣魚網站。為了規避自動化沙箱檢測，攻擊者利用Captcha進行驗證，經人工確認後才會顯示頁面內容。此時，攻擊者採用將網頁背景模糊化的頁面，誘導收件人輸入個人資料，再根據收件人所輸入的公司域名，動態生成相應的登入頁面，包含公司商標和相關背景圖，以增加網頁真實性，欺騙收件人是合法的系統登入介面。圖1為此攻擊手法之流程圖。


圖1：利用Captcha進行驗證，偽造登入系統頁面。
資料來源：TWCERT/CC整理

TWCERT/CC與國家資通安全研究院近期亦觀察到駭客通過模仿公務機關名義發送社交工程郵件，試圖竊取企業與個人的敏感資訊，如近期駭客偽冒財政部或稅務機關發送涉及稅務事宜的電子郵件、偽冒勞動部發送勞工退休相關事宜的電子郵件等。


圖2：駭客偽冒財政部發送稅務事宜之釣魚郵件

辨識來自公務機關的電子郵件變得至關重要，防範此類攻擊，可採取以下幾點：

1. 域名驗證：檢查郵件的發送者域名是否為官方的政府域名，如「.gov」或「.gov.tw」。即使域名看似合法，也要注意細節，駭客可能使用相似的字符進行欺騙，如「.g0v」、「.gov.tw1」等類似域名誘導使用者。
2. 郵件內容分析：官方郵件通常會提供明確的指示和聯絡方式，若要求執行重要操作，可直接聯繫相關政府門進行確認，勿隨便點擊郵件中的連結。此外，若是正式文件通常會使用實體公文書信掛號，並非以電子郵件形式通知。
3. 防護措施：安裝並定期更新防毒軟體，確保病毒碼隨時保持更新，攔截並過濾可疑郵件。
4. 加強宣導：企業需定期對員工進行資安教育，提高對社交工程攻擊的認識和防範能力。

TWCERT/CC提醒民眾在接獲相關電子郵件時，應特別注意寄件者來源是否正常，以防範潛在的網路攻擊。此外，駭客經常變造惡意網址，如org.tw則改成0rg.tw，提高攻擊成功率，在點擊信件連結時，應再確認網址正確性。民眾應提高警覺，避免隨意點擊不明連結，以確保個人與企業資訊安全。

# 第 2 章、國內外重要資安事件

## 2.1 新興應用資安

### 2.1.1 惡意AI模型潛伏Hugging Face，駭客陰謀大揭秘


Hugging Face成立於2016年，是全球AI領域最重要的開源平台，以豐富AI模型和資料庫聞名。近期ReversingLabs（RL）的威脅研究團隊發現Hugging Face平台上存在惡意機器學習模型，這些模型利用Python的Pickle檔案序列化漏洞執行惡意程式碼，並將其隱藏在模型中。然而Hugging Face的安全掃描機制並未將其標記為「不安全」，研究人員將這種傳播技術命名為「nullifAI」，引發了對AI模型安全性的廣泛注意。

Pickle是python的一個標準函式庫，主要用於序列化和反序列化Python物件結構，特別在機器學習模型的資料儲存和傳輸中方便使用。雖然Pickle易於使用，但它常見的序列化漏洞風險使得攻擊者可透過Pickle將惡意程式碼隱藏在模型中。Hugging Face官方特別提醒使用Pickle時，應格外注意資安風險，並將Pickle序列化的問題稱為

「Pickling」。

Hugging Face平台提供名為「picklescan」的掃描工具，專門用於檢測惡意的Pickle檔案。不過該工具僅能掃描完整、未損壞的Pickle檔案，因此駭客利用「損壞」Pickle檔案的技術規避安全檢測，這些損壞的檔案在反序列化時會出現錯誤，但不影響執行惡意程式碼。圖3和圖4是ReversingLabs威脅研究團隊發現的惡意AI模型，目前已被Hugging Face平台關閉。

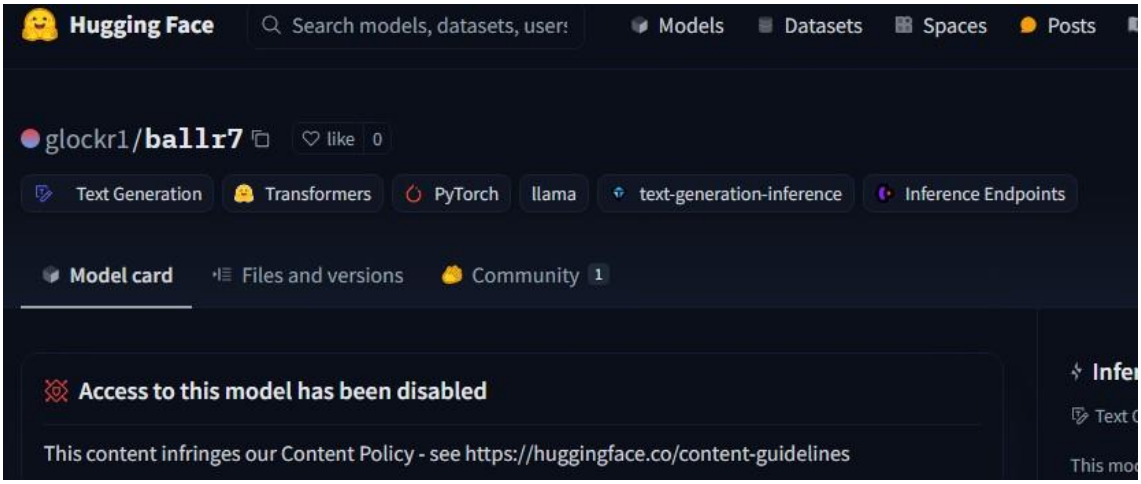


圖3: 在Hugging Face上的惡意AI模型。

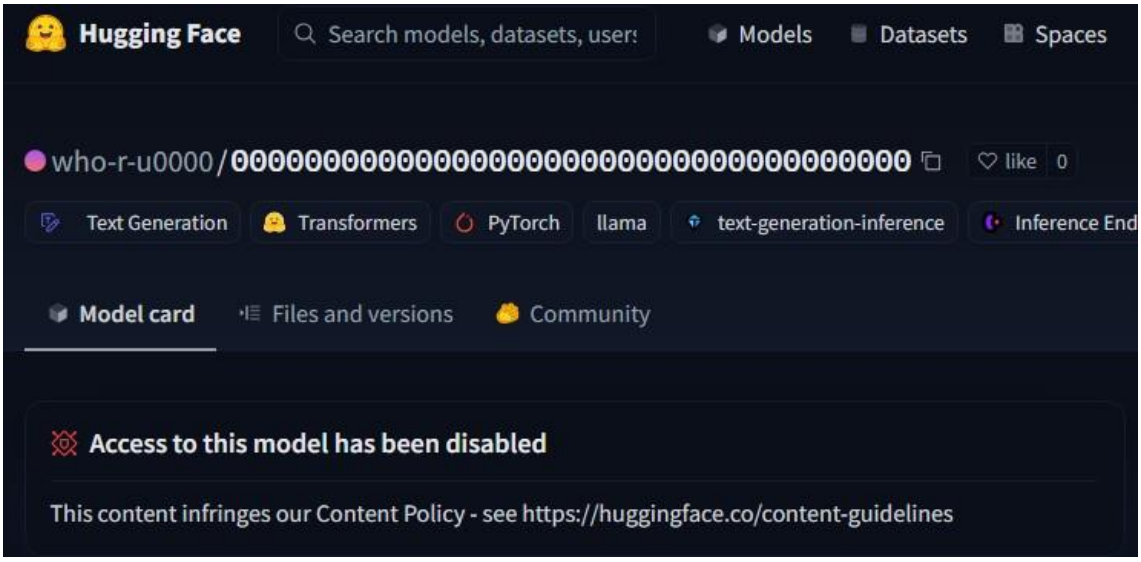


圖4: 在Hugging Face上的惡意AI模型。

駭客建構的AI模型使用壓縮格式的Pickle檔案，檔案的前半段包含惡意程式碼，後半段則是無效或損壞的資料。在解序列化的過程中，由於檔案逐步被處理，因此位於前半段的惡意程式碼會先被成功執行，由於後半段的資料損毀，反序列化過程中出現錯誤並終止執行。由於picklescan僅能掃描完整、未損壞的Pickle檔案，因此無法識別此AI模型是惡意的Pickle檔案。

2025年1月20日，ReversingLabs向Hugging Face通報該平台上發現惡意AI模型與工具漏洞。Hugging Face團隊於24小時內移除惡意模型，並將picklescan進行更新，以加強「損壞」的Pickle檔案的偵測能力。

針對使用開源AI模型的防禦建議如下：

1. 開發團隊在使用 Hugging Face 等平台上的機器學習模型時，應格外小心 Pickle檔案。
2. 建議避免使用Pickle檔案格式，改用其他較安全的序列化檔案格式。
3. 確保任何載入AI模型所需的自訂操作與序列化的模型資料分開。

惡意AI模型的IoC：

- 1733506c584dd6801accf7f58dc92a4a1285db1f
- 79601f536b1b351c695507bf37236139f42201b0
- 0dcc38fc90eca38810805bb03b9f6bb44945bbc0
- 85c898c5db096635a21a9e8b5be0a58648205b47
- 107.173.7.141

- 相關連結
  1. FBI Denver Warns of Online File Converter Scam

## 2.2 資安趨勢

### 2.2.1 勒索軟體威脅升溫，攻擊手法日趨複雜


近期，勒索軟體攻擊事件在全球範圍內持續升溫，台灣也成為駭客攻擊的目標之一。多個行業陸續傳出遭攻擊的案例，包括醫療機構、學校及上市櫃公司等。根據研究，駭客組織Crazyhunter、Nightspire及UAT-5918等，已在台灣發動數起攻擊，對相關機構的資訊安全造成嚴重威脅。

根據 CYFIRMA的研究報告，2025 年 2 月全球勒索軟體攻擊事件急遽攀升，總計高達 956 起，較 1 月增加了 87%。其中，以 Clop 勒索軟體集團最為活躍，受害案例達 332 起；而 Play 勒索軟體的攻擊範圍與規模亦愈來愈大。

報告指出，在歐洲地區，特別是醫療保健產業，攻擊者已開始利用 Check Point 網路閘道的漏洞(CVE-2024-24919)進行攻擊，並部署 PlugX 與 ShadowPad 惡意程式，再透過 NailaoLocker 進行勒索。部分駭客組織也針對亞洲特定產業展開攻擊行動。例如，Emperor Dragonfly 便對一家亞洲軟體公司發動 RA World 勒索軟體攻擊，並勒索 200 萬美元。該組織自 2024 年中至 2025 年初間，亦針對東南

歐及亞洲政府機構與電信業者發動攻擊。

**2025 年 2～3 月勒索軟體攻擊趨勢**

- 全球勒索軟體攻擊數量大幅上升，製造業與醫療保健產業受害情況尤為嚴重。
- 攻擊者持續利用已知漏洞(CVE-2024-24919)，對歐洲醫療機構進行滲透攻擊。
- 勒索手法日趨複雜，結合偽裝文件與雙重勒索策略(Double Extortion)。

**攻擊台灣之駭客組織活動概況**

近期，台灣成為多個駭客組織的攻擊目標，這些組織利用勒索軟體對企業發動攻擊，造成重大的資訊安全的影響，其中駭客組織Crazyhunter、Nightspire及UAT-5918針對各行各業進行網路攻擊，並要求高額贖金。這些攻擊不僅對企業構成威脅，也引發各界對資安防護與風險管理的廣泛關注。

Crazyhunter 此勒索軟體集團近期針對台灣醫療機構頻繁發動攻擊，導致系統癱瘓與個資外洩。其攻擊模式結合「極速滲透與防禦突破」(Ultra-fast attack approach)與「三維資料殲滅系統」(Three-dimensional Data Annihilation System)，並運用 AI 及深度偽造技術強化攻擊與製造虛假證據。近期發現攻擊者透過破解帳號的弱密碼，並利用 Active Directory(AD)設定錯誤的漏洞，成功入侵內部系統，接著使用「自帶驅動程式攻擊(Bring Your Own Vulnerable Driver, BYOVD)」的手法，包括植入修改過的 Zemana 驅動程式，來繞過資安防護機制、取得更高權限。隨後，攻擊者透過群組原則(GPO)在內部網路橫向移動，將惡意程式散布到重要的系統中，對內部資料進

行加密，並且向受害單位進行勒索。自 2025 年 3 月初以來，已對台灣三個不同產業發動攻擊，嚴重衝擊醫療服務與資料安全。

Nightspire Nightspire為新興駭客組織，擅長透過暗網入口網站結合心理恐嚇手法實施雙重勒索。攻擊手法包括入侵系統、竊取敏感資料並加密，再以公開洩漏資料為威脅向受害者索取贖金。其資料洩漏網站(Data Leak Site, DLS)會列出受害者清單，並顯示資料公開倒數計時器。近期已公布多起香港與台灣企業的攻擊事件，造成敏感資訊外洩，對業務運作與客戶資料安全造成嚴重威脅。

UAT-5918 針對台灣關鍵基礎設施攻擊的 APT 組織，自 2023 年起針對台灣關鍵基礎設施展開滲透行動，目標產業包括電信、醫療保健及資訊科技等。其主要手法為利用 N-day 漏洞取得初始存取權限，進一步透過開源工具(如 FRPC、FScan、Earthworm)與 Web Shell 技術竊取使用者憑證並建立後門，以進行長期監控與資料竊取。

隨著勒索軟體攻擊日益複雜且具針對性，政府與企業必須加強資安防禦措施，尤其是關鍵基礎設施與高風險行業。建議重點如下：

- 強化漏洞管理與修補機制，避免成為攻擊跳板。
- 提升事件應變能力，確保一旦發生攻擊能快速復原。
- 深化威脅情報分析與即時監控機制，提前掌握潛在威脅。

透過持續監測、主動防禦與全面資安策略，以降低勒索軟體所帶來的營運風險與損失。

● 相關連結

1. TRACKING RANSOMWARE – FEBRUARY 2025
2. Crazyhunter: The Ransomware with the Three-Dimensional Data Annihilation System That Redefines Da
3. UAT-5918 APT group targets Taiwan critical infrastructure, possible linkage to Volt Typhoon

## 2.3 國際政府組織資安資訊

### 2.3.1 FBI發出安全警示，駭客利用免費轉檔網站散佈惡意軟體


近期美國聯邦調查局(Federal Bureau of Investigation, FBI)發布警告，提醒民眾注意一項日益嚴重的攻擊手法。網路犯罪分子利用免費線上轉檔工具散佈惡意軟體，這些工具表面提供文件、圖片或影音格式的轉換服務，實際上可能將惡意程式隱藏在下載的檔案中，導致使用者的個人資料與設備安全構成威脅。

攻擊者利用設計精巧、看似正常的網站或應用程式，這些網站或應用程式通常提供免費的文件轉換及編輯工具，像是將Word檔案轉換為PDF、將多張圖片合併成PDF，甚至提供影音檔案下載等服務。網站服務或程式多宣稱能簡化日常工作流程或免費提供服務，吸引大量使用者上網搜尋使用。然而，當使用者下載並開啟這些已轉檔的檔案時，該檔案可能隱藏惡意程式或勒索病毒，一旦使用者開啟檔案即感染設備。

除了已轉檔的文件可能含有惡意程式外，攻擊者也可能擷取檔案中的資料，如個資、銀行資料、加密貨幣帳戶訊息、電子郵件地

址、帳號密碼等敏感資料，對受害者的隱私和財務等造成危害。o

雖然免費線上轉檔工具十分方便，若無法確保其網站的安全性，這些工具也可能成為攻擊者的陷阱。FBI表示此類攻擊的受害者直到遭遇勒索病毒攻擊或是財務詐騙後，才發現設備已被惡意軟體感染，FBI也鼓勵此類騙局的受害者向美國聯邦調查局網路犯罪投訴中心(www[.]ic3[.]gov)舉報，通報不僅能幫助追蹤亦可協助其他使用者受害。

為了減少成為受害者的風險，以下是幾項建議措施：

1. 避免使用不明來源的免費工具，尤其是未經過驗證的網站。選擇官方或知名平台提供的軟體服務，並儘可能使用本地端的專業軟體處理敏感文件。
2. 保持防毒軟體的最新狀態，並確保定期進行掃描，避免惡意程式進入系統。尤其開啟任何檔案前，務必執行病毒掃描。
3. 如發現設備異常或有中毒跡象，應立刻斷開網路並採取相應行動。例如使用可信任的乾淨設備更改所有密碼，並啟用雙因子認證(2FA)增加帳號安全性。
4. 若已成為受害者，可向相關單位回報和尋求專業協助。

隨著網路攻擊手法的日益精細，網路使用者必須保持高度警覺，尤其是在使用免費工具或下載文件。具備基本的安全意識與防範措施，才能最大程度減少遭受攻擊的風險，保障自己的隱私安全與個人資產。

● 相關連結

1. FBI Denver Warns of Online File Converter Scam

## 2.4 軟硬體漏洞資訊

### 2.4.1 Broadcom 旗下 Vmware 虛擬化軟體存在重大資安漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2025-22224 |
| **影響產品** | Vmware |
| **解決辦法** | 更新至以下版本：<br>Vmware ESXi 7.0 ：ESXi70U3s-24585291<br>Vmware ESXi 8.0 ：ESXi80U2d-24585300 或 ESXi80U3d-24585383<br>Vmware Workstation 17.6.3<br>Vmware Cloud Foundation 4.5.x：ESXi70U3s-24585291<br>Vmware Cloud Foundation 5.x：ESXi80U3d-24585383<br>VMware Telco Cloud Platform 5.x , 4.x , 3.x , 2.x：依官方文件指示進行更新 |

- 內容說明：

  Broadcom 針對旗下多個 Vmware 虛擬化軟體產品發布重大資安漏洞(CVE-2025-22224，CVSS：9.3)。此漏洞為檢查時間及使用時間(TOCTOU)，可能導致越界寫入(Out-of-Bounds Write)，若攻擊者取得虛擬機的本機管理權限，則有機會透過 VMX 處理程序，在主機執行任意程式碼。

- 影響平台：
  - Vmware ESXi 7.0
  - Vmware ESXi 8.0
  - Vmware Workstation 17.x
  - Vmware Cloud Foundation 4.5.x
  - Vmware Cloud Foundation 5.x
  - VMware Telco Cloud Platform 5.x , 4.x , 3.x , 2.x
- 資料來源：

1. CVE-2025-22224
2. VMSA-2025-0004: VMware ESXi, Workstation, and Fusion updates address multiple vulnerabilities

## 2.4.2 Fortinet 旗下 FortiADC 存在重大資安漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2023-37933 |
| **影響產品** | FortiADC |
| **解決辦法** | 更新至以下版本：<br>FortiADC 7.4.1(含)之後版本<br>FortiADC 7.2.2(含)之後版本<br>FortiADC 7.1.4(含)之後版本<br>其餘版本請更新至固定版本 |

- 內容說明：

  Fortinet 的 FortiADC 是一款應用程式交付控制器，旨在增強應用程式的擴展性、效能及安全性。Fortinet 發布 FortiADC GUI 存在重大資安漏洞(CVE-2023-37933，CVSS：8.8)，此漏洞允許經過身分驗證的攻擊者，透過特殊的 HTTP 或 HTTPs 執行跨腳本攻擊(XSS)。

- 影響平台：
  - FortiADC 7.4.0
  - FortiADC 7.2.0 至 7.2.1
  - FortiADC 7.1.0 至 7.1.3
  - FortiADC 7.0 所有版本
  - FortiADC 6.2 所有版本
  - FortiADC 6.1 所有版本
  - FortiADC 6.0 所有版本
  - FortiADC 5.4 所有版本
  - FortiADC 5.3 所有版本
- 資料來源：
  1. XSS flaw in Fortiview/SecurityLogs pages
  2. CVE-2023-37933

## 2.4.3 Fortinet 旗下 FortiSandbox 存在重大資安漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2024-52961 |
| **影響產品** | FortiSandbox |
| **解決辦法** | 更新至以下版本：<br>FortiSandbox 5.0.1 (含)之後版本<br>FortiSandbox 4.4.7 (含)之後版本<br>FortiSandbox 4.2.8 (含)之後版本<br>FortiSandbox 4.0.6 (含)之後版本<br>其餘版本請更新至固定版本 |

- 內容說明：

  FortiSandbox 是 Fortinet 旗下一款威脅防護解決方案，可執行動態分析以識別先前未知的網路威脅。Fortinet 發布 FortiSandbox 存在重大資安漏洞(CVE-2024-52961，CVSS：8.8)，此漏洞存在 FortiSandbox 作業系統命令的特殊符號設計不當，可允許經過身分驗證且具有讀取權限的攻擊者，透過特殊的請求執行未經授權指令。

- 影響平台：
  - FortiSandbox 5.0.0
  - FortiSandbox 4.4.0 至 4.4.6
  - FortiSandbox 4.2.0 至 4.2.7
  - FortiSandbox 4.0.0 至 4.0.5
  - FortiSandbox 3.2 所有版本
  - FortiSandbox 3.1 所有版本
  - FortiSandbox 3.0 所有版本
- 資料來源：

  1. Os command injection on vm download feature
  2. CVE-2024-52961

## 2.4.4 Fortinet 旗下 FortiIsolator 存在重大資安漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2024-55590 |
| **影響產品** | FortiIsolator |
| **解決辦法** | 將 FortiIsolator 更新至 2.4.6 (含)之後版本 |

- 內容說明：

  FortiIsolator 是 Fortinet 旗下的一款遠端瀏覽器隔離解決方案，允許用戶在隔離的環境中安全瀏覽網路和安全內容。Fortinet 發布 FortiIsolator 存在重大資安漏洞(CVE-2024-55590，CVSS：8.8)，該漏洞存在 FortiIsolator 作業系統命令的特殊符號設計不當，可允許經過身分驗證且具有讀取管理員權限和 CLI 訪問權限的攻擊者，透過特殊的 CLI 命令執行未經授權的指令。

- 影響平台：
  - FortiIsolator 2.4.0 至 2.4.5
- 資料來源：

  1. Multiple command injections on CLI
  2. CVE-2024-55590

## 2.4.5 GitLab 的社群版(CE)及企業版(EE)存在2個重大資安漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2025-25291,CVE-2025-25292 |
| **影響產品** | GitLab CE/EE |
| **解決辦法** | 將 GitLab CE/EE 更新至 17.7.7、17.8.5、17.9.2(含)之後版本 |

- 內容說明：

  GitLab 是基於 Git 的整合軟體開發( DevSecOps )平台，提供版本控制、CI/CD 自動化等功能。近期 GitLab 針對社群版(CE)及企業版(EE)發布多個資安漏洞公告並提供修補版本，其中以 CVE-2025-25291(CVSS 4.x：8.8) 與 CVE-2025-25292(CVSS 4.x：8.8)為重大資安漏洞，這二個繞過身分驗證漏洞存在 ruby-saml 的程式庫，攻擊者能存取已經過身分驗證且有效簽署的 SAML 檔，作為另一個有效使用者進行身分驗證。

- 影響平台：
  - GitLab CE/EE
- 資料來源：

  1. GitLab Critical Patch Release: 17.9.2, 17.8.5, 17.7.7
  2. CVE-2025-25291
  3. CVE-2025-25292

## 2.4.6 Fortinet 旗下 FortiManager 存在作業系統命令漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2024-46662 |
| **影響產品** | FortiManager |
| **解決辦法** | 更新 Cisco ISE 3.1P10 (含)之後版本<br>更新 Cisco ISE 3.2P7 (含)之後版本<br>更新 Cisco ISE 3.3P4 (含)之後版本<br>Cisco ISE 3.0 請遷移至固定版本 |

- 內容說明：

  FortiManager 是 Fortinet 旗下的一款具有多功能網路安全管理產品，提供單一管理介面、集中管理和監控網路等。Fortinet 發布 FortiManager 存在重大資安漏洞(CVE-2024-46662，CVSS：8.8)，此漏洞為作業系統命令的特殊符號設計不當，可允許經過身分驗證的攻擊者，透過特殊的封包執行未經授權的命令。

- 影響平台：
  - FortiManager Cloud 7.4.1 至 7.4.3
  - FortiManager 7.4.1 至 7.4.3
- 資料來源：

  1. Command injection in csfd daemon
  2. CVE-2024-46662

## 2.4.7 Veeam旗下Veeam Backup & Replication備份軟體存在重大資安漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2025-23120 |
| **影響產品** | Veeam Backup & Replication |
| **解決辦法** | 將 Veeam Backup & Replication 更新至 12.3.1.1139 (含)以後版本 |

- 內容說明：

  Veeam Backup & Replication 是 Veeam 核心備份軟體，近日 Veeam 發布重大資安漏洞公告。此漏洞(CVE-2025-23120，CVSS：9.9)允許經網域驗證的使用者，可遠端執行程式碼。

- 影響平台：
  - Veeam Backup & Replication 12.3.0.310 (含)之前所有 12.x 版
- 資料來源：

  1. veeam_CVE-2025-23120
  2. CVE-2025-23120

## 2.4.8 Kubernetes 的 ingress-nginx 存在多個重大資安漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2025-24514,CVE-2025-1097,CVE-2025-1098,CVE-2025-1974 |
| **影響產品** | Kubernetes ingress-nginx |
| **解決辦法** | 更新至以下版本：<br>Kubernetes ingress-nginx 1.11.5<br>Kubernetes ingress-nginx 1.12.1 |

- 內容說明：

  Kubernetes (K8s)是由 Google 設計用來自動化部屬、擴展與管理容器化的系統，可以集群的方式運行和管理容器，實現高效率的建置。近日揭露 Kubernetes 的 ingress-nginx 存在四個重大資安漏洞。

  【CVE-2025-24514，CVSS：8.8】

  此漏洞為 auth-url 的註解可注入至 nginx，可能導致在 ingress-nginx 控制器的上下文中執行任意程式碼，並洩漏控制器存取的資料。

  【CVE-2025-1097，CVSS：8.8】

  此漏洞為 auth-tls-match-cn 的註解可注入至 nginx，可能導致在 ingress-nginx 控制器的上下文中執行任意程式碼，並洩漏控制器存取的資料。

  【CVE-2025-1098，CVSS：8.8】

  此漏洞為 mirror-target 和 mirror-host 的註解可注入至 nginx，可能導致在 ingress-nginx 控制器的上下文中執行任意程式碼，並洩漏控制器存取的資料。

  【CVE-2025-1974，CVSS：9.8】

此漏洞允許未經過身分驗證的攻擊者可存取 Pod 網路，在 ingress-nginx 控制器的上下文中執行任意程式碼，可能導致洩漏控制器的資料。

- 影響平台：
  - Kubernetes ingress-nginx 1.11.0 之前版本
  - Kubernetes ingress-nginx 1.11.0 - 1.11.4
  - Kubernetes ingress-nginx 1.12.0
- 資料來源：

1. CVE-2025-24514: ingress-nginx controller
2. CVE-2025-1097: ingress-nginx controller
3. CVE-2025-1098: ingress-nginx controller
4. CVE-2025-1974: ingress-nginx admission controller RCE escalation
5. CVE-2025-24514
6. CVE-2025-1097
7. CVE-2025-1098

# 第 3 章、資安研討會及活動

- **資安研討會**

| 【資安學院】4/26、5/3 iPAS-「初級」資訊安全工程師-能力研習衝刺班 | |
|---|---|
| 活動時間 | 2025-04-26 09:00 ~ 16:00、2025-05-03 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/5420 |
| 活動概要 |  <br>**【費用】**<br>原價：11,000元/人<br>軟協會員：8,500元/人<br>(可單科報名，請洽承辦人)<br>費用含稅、教材、餐點及完課證明，不包含考試費用，請自行上網報名。<br>報名截止： 2025-04-22<br>**【活動內容 / Event Deails】**<br>使學員瞭解資訊安全管理與技術專有名詞及其代表意義，並具備資訊安全管理基礎，另亦統整資訊安全技術之基礎知識，透過講師授課，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】中華民國資訊軟體協會<br>【聯絡窗口】02-2553-3988 分機 816 林專員<br>security@cisanet.org.tw |
| 【資安學院】5/7 網路安全檢測實務-實作課 | |
| 活動時間 | 2025/05/07 |
| 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/5470 |
| 活動概要 |  <br>【費用】<br>原價：8,300元/人<br>早鳥價：7,800元/人(開課前一個月)<br>軟協會員：7,200元/人<br>費用含稅、教材、餐點及完課證明<br>報名截止： 2025-05-02<br>【活動內容 / Event Deails】<br>專為對網站資安有興趣的資訊與資安人員設計，提供學員全面了解網站常見的安全威脅，並掌握有效的檢測技術與實務操作，瞭解 OWASP Top 10 的檢測技術。深入解析網站常見的資安問題、業界廣泛使用的安全檢測技術與工具，進行實務演練，結合理論與實際操作，讓參與者熟悉漏洞檢測流程，提升網站安全防護能力。 |

| | |
|---|---|
| | **【主辦單位】中華民國資訊軟體協會**<br>**【聯絡窗口】02-2553-3988 分機 816 林專員**<br>**security@cisanet.org.tw** |
| **【資安學院】5/9 勒索病毒攻擊案例研習** | |
| **活動時間** | **2025/05/09** |
| **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/5413** |
| **活動概要** |  <br>**【費用】**<br>原價：4,000元/人<br>早鳥價：3,800元/人(開課前一個月)<br>軟協會員：3,500元/人<br>費用含稅、教材及完課證明<br>報名截止： 2025-05-05<br>**【活動內容 / Event Deails】**<br>勒索病毒攻擊為當前政府企業遭受資安攻擊的主流攻擊手法之一，其原理係將主機檔案進行加密，受害者需支付一定贖金取得解密金鑰解開遭勒索病毒加密的檔案。勒索病毒攻擊往往造成資訊系統之停擺，對政府企業危害甚大。本課程旨在分析勒索病毒運作之原 |

| | |
|---|---|
| | 理、針對勒索病毒攻擊之防範及應變處理進行介紹，並援引實務案例進行研討。<br>**【主辦單位】中華民國資訊軟體協會**<br>**【聯絡窗口】02-2553-3988 分機 816 林專員**<br>security@cisanet.org.tw |
| **【資安學院】5/23資安法報給你知—探現今資安政策與機關稽核實務** | |
| **活動時間** | **2025/05/23** |
| **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/5419** |
| **活動概要** |  <br>**【費用】**<br>原價：7,200元/人<br>早鳥價：6,800元/人(開課前一個月)<br>軟協會員：6,200元/人<br>費用含稅、教材、餐點及完課證明<br>報名截止： 2025-05-16<br>**【活動內容 / Event Deails】**<br>資通安全管理法自 108 年施行，資通安全稽核已成為納管對象所應辦理的重要法遵事項之一，資通安全管理法也在 112 年起開始進行修法作業。本次課程將介紹資通安全管理法之重點內容，包括母法 |

| | |
|---|---|
| | 及其 6 項子法、維護計畫、防護基準等；同時說明資通安全管理法主管機關所辦理資通安全實地稽核的方式、重點及常見問題。**【主辦單位】中華民國資訊軟體協會**<br>**【聯絡窗口】02-2553-3988 分機 816 林專員**<br>**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：**

| 一等一科技 U-Office Force - Improper Authentication | |
|---|---|
| **TVN / CVE ID** | TVN-202503002 / CVE-2025-2395 |
| **CVSS** | 9.8 (Critical)<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | U-Office Force 28.0(不含)以前版本 |
| **問題描述** | 一等一科技U-Office Force存在Improper Authentication漏洞，未經身分鑑別之遠端攻擊者在利用特定API時，透過竄改cookie可用管理員身分進行登入。 |
| **解決方法** | 更新至28.0(含)以後版本 |
| **公開日期** | 2025-03-17 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-10011-3de72-1.html** |
| **一等一科技 U-Office Force - Arbitrary File Upload** | |
| **TVN / CVE ID** | TVN-202503003 / CVE-2025-2396 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | U-Office Force 28.0(不含)以前版本 |
| **問題描述** | 一等一科技U-Office Force存在Arbitrary File Upload漏洞，已取得一般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** | 更新至28.0(含)以後版本 |
| **公開日期** | 2025-03-17 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-10013-0d371-1.html** |

| 商之器科技 EBM Maintenance Center - SQL injection | |
|---|---|
| **TVN / CVE ID** | TVN-202503004 / CVE-2025-2585 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | EBM Maintenance Center 25.04.31435(不含)以前版本 |
| **問題描述** | 商之器科技EBM Maintenance Center存在SQL Injection漏洞，已取得一般權限之遠端攻擊者可注入任意SQL指令以讀取、修改及刪除資料庫內容。 |
| **解決方法** | 更新至25.04.31435(含)以後版本 |
| **公開日期** | 2025-03-21 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-10021-8786e-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3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/**