TWCERT/CC 資安情資電子報

2025 年 4 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

開源 GitHub 專案 ChatGPT 漏洞遭大規模濫用，美國為主要攻擊目標

資安業者Veriti的研究員發現一個正被積極利用的伺服器端請求偽造（SSRF）漏洞，編號為CVE-2024-27564（CVSS：6.5）。此漏洞允許攻擊者利用ChatGPT(基於 PHP開源GitHub 專案)的pictureproxy.php元件（commit ID為f9f4bbc），通過「url」參數發起任意請求，繞過安全控制，控制ChatGPT請求指定資源，從而可能導致敏感資訊洩漏。

伺服器端請求偽造（SSRF, Server-Side Request Forgery）是一種網路安全漏洞，攻擊者利用應用程式的請求功能，使伺服器發送惡意請求到未經授權的內部或外部資源。這種攻擊通常發生在應用程式允許用戶提供 URL 請求遠端資源，但沒有適當驗證的情況下，攻擊者可利用SSRF漏洞存取企業內部資源、繞過IP限制、對內網發動攻擊等。

這一漏洞正被超過一萬個IP位址積極利用，對全球多個組織造成影

響。主要受影響的行業是金融業，美國是受影響最大的國家，占比達到33%。其他受影響的國家包括德國和泰國，各占7%；此外，醫療照護與政府機關亦是受影響的領域。圖 1 是Veriti偵測到CVE-2024-27564漏洞攻擊的區域分布圖。

圖1: Veriti 公司偵測到主要的受駭地區

儘管這一漏洞被歸類為中等風險，但受害的組織主要是因為入侵防禦系統(IPS)、Web應用程式防火牆(WAF)和防火牆設置不當所引起。企業通常會積極修補高風險等級的漏洞，而忽略中低程度風險的漏洞。然而，Veriti研究員強調：「沒有任何漏洞小到可以忽略不計，攻擊者會利用他們能找到的任何弱點。」

此連結(https://www.youtube.com/watch?v=R9zsRGYc2PA)是Veriti公司提供的攻擊演示的影片。為了防範此類攻擊，資安團隊應定期檢查入侵防禦系統、Web 應用程式防火牆 和防火牆配置，以確保系統受到充分的保護，可以抵禦外來攻擊。

以下是目前偵測到的攻擊者 IP 地址：

31.56.56[.]156

38.60.191[.]7
94.156.177[.]106
159.192.123[.]90
119.82.255[.]34
103.251.223[.]127
104.143.229[.]115
114.10.44[.]40
116.212.150[.]192
145.223.59[.]188
167.100.106[.]99
174.138.27[.]119
212.237.124[.]38
216.158.205[.]221

- 相關連結

1. OpenAI Under Attack: CVE-2024-27564 Actively Exploited in the Wild
2. CVE-2024-27564 - SSRF & LFI

第 2 章、國內外重要資安事件

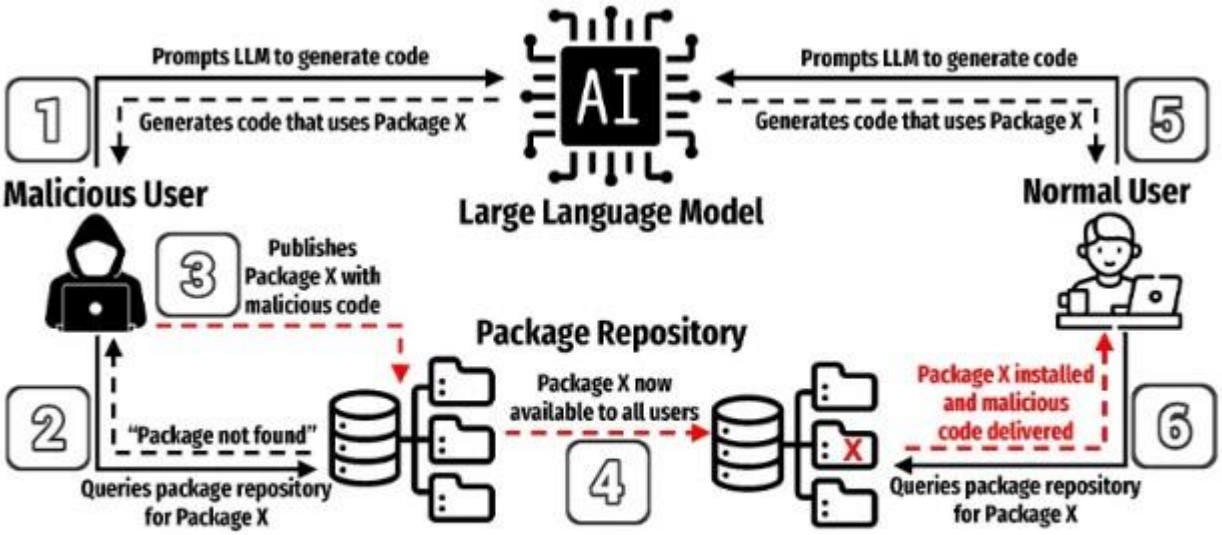
2.1 新興應用資安

2.1.1 不存在的套件，真實的威脅：LLM 誤導開發者走入 Slopsquatting 陷阱

近年來開發人員在程式開發過程中，時常依賴大型語言模型(LLM)生成的程式碼進行編譯與整合。然而，這些AI模型經常「幻想」不存在的程式碼和函式庫，且這類幻覺具有一定程度的重複性與規律性。資安研究員Seth Larson為此創造「slopsquatting」一詞，專指利用錯誤的函式庫名稱發動的攻擊。若攻擊者針對AI模型所「幻想」的虛假函式庫進行精心設計並發布相應的惡意套件，誘使開發人員將其載入專案中，進而引發嚴重的供應鏈攻擊與軟體安全風險。

此研究由UTSA博士生Joe Spracklen領導，聚焦於LLM在程式碼生成過程中頻繁產生不安全或不存在的函式庫名稱問題，並已投稿於USENIX 2025資安研討會。研究團隊利用二組獨特的資料集，針對包含GPT-4、Claude、CodeLlama、DeepSeek Coder及Mistral等多款主流AI模型進行實驗，收集576,000筆Python與JavaScript程式碼範例。研究結果顯示，將近20%函式庫並不存在，且這些幻想的函示庫名稱被AI模型反覆

生成。圖1為此篇論文內敘述如何利用LLM幻覺產生函式庫之流程圖。



How to exploit package hallucination (Source: Arxiv)

圖1: 利用LLM幻覺產生的函式庫之流程圖，圖片來源：Arxiv

為了驗證LLM是否會反覆生成相同的幻覺套件名稱，研究團隊選取500個提示的隨機樣本，並對每個提示進行10次重複查詢。實驗結果顯示，43%的幻覺套件在所有重複查詢中均被持續生成；39%的幻覺套件則未在重複查詢中再次出現。此外，有58%的情況下，幻覺套件會在多次查詢中重複出現，進一步證實LLM生成虛假套件名稱的頻繁且具有規律性的特徵。

根據研究數據顯示，在利用AI模型生成的程式碼中，Python相較於JavaScript出現幻覺套件的比例較低；另外，在各類的AI模型中，GPT系列模型生成的幻覺套件數量少於其他開源AI模型。

研究人員建議開發人員使用AI模型生成程式碼時，務必自行檢查AI所提供的程式碼及其函式庫，避免誤用攻擊者精心設計的惡意程式庫。

切勿盲目相信AI輸出的內容，才能有效降低遭受供應鏈攻擊及其他資安風險的可能性。

- 相關連結
  1. Package hallucination: LLMs may deliver malicious code to careless devs
  2. UTSA researchers investigate AI threats in software development
  3. We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLM

2.2 軟體系統資安議題

2.2.1 Oracle雲端服務驚傳資料外洩，疑似使用舊漏洞CVE-2021-35587

近期駭客論壇BreachForums出現名為rose87168的用戶，宣稱可存取Oracle 雲端伺服器並出售敏感資料，包含單一登入(Single Sign-on，SSO)憑證、輕型目錄存取協定(Lightweight Directory Access Protocol，LDAP)帳密、OAuth2金鑰和客戶資訊。由於這些敏感資料可能導致大規模供應鏈攻擊，引起各方關注。儘管Oracle公開否認，但新加坡資安業者CloudSEK進行深入了解後，提供免費工具供大眾檢查是否為潛在受影響對象。

CloudSEK 的研究報告顯示，駭客透過成功攻擊「login[.]us2[.]oraclecloud[.]com」子網域並建立文件做為攻擊證據。根據圖2 Wyback Machine紀錄顯示，該網域伺服器為Oracle Fusion Middleware 11G，且從情資得知該服務存在弱點CVE-2021-35587(CVSS：9.8)，影響代理程式元件OpenSSO Agent，受影響版本包含11.1.2.3.0、12.2.1.3.0和12.2.1.4.0。而此在攻擊發生前幾週，目標伺服器已被Oracle關閉。

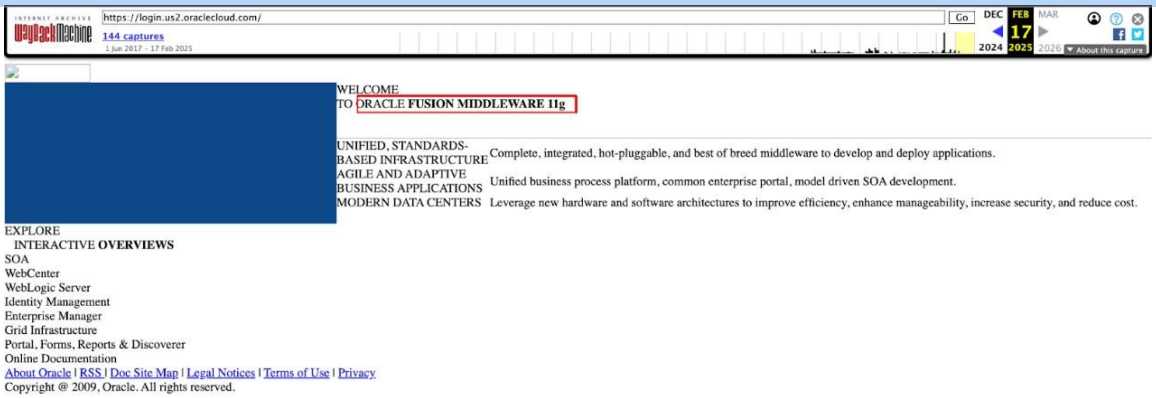


圖2 Wayback Machine的login[.]us2[.]oraclecloud[.]com紀錄。圖片來源：CloudSEK

根據此次事件，CloudSEK提出三項關鍵證據證明，外洩資料確有關用戶實際資料，而非單純只是測試資料：

- **證據1 -「login[.]us2[.]oraclecloud[.]com」目的**

CloudSEK 在 Oracle 官方 Github 儲存庫發現與「login[.]us2[.]oraclecloud[.]com」相關OAuth2流程腳本。此腳本使用「客戶端憑證授予」的方式驗證API請求，再利用client_id和secret_key（Base64 編碼）產生token向URL發送POST請求，接著該token 會做為授權標頭，用於後續API請求中的Bearer token。證明該伺服器為正式環境並非測試或臨時環境。

```
with open(creds_file, 'r') as stream:
    creds = yaml.safe_load(stream)

auth_string = creds['client_id']
auth_string += ':'
auth_string += creds['secret_key']

encoded = base64.b64encode(auth_string.encode('ascii'))
encoded_string = encoded.decode('ascii')

token_url = 'https://login.us2.oraclecloud.com:443/oam/oauth2/tokens?grant_type=client_credentials'

auth_headers = {}
auth_headers['Content-Type'] = 'application/x-www-form-urlencoded'
auth_headers['charset'] = 'UTF-8'
auth_headers['X-USER-IDENTITY-DOMAIN-NAME'] = 'usoracle30650'
auth_headers['Authorization'] = f'Basic {encoded_string}'

r = requests.post(token_url, headers=auth_headers)
```

```
from time import gmtime, strftime
import datetime
import requests
import base64
import yaml
import json
import os.path
import re
import pprint

api_url = 'https://ocm-apis-cloud.oracle.com/'
picCompartmentOcid = 'ocid
picTenancyId = '
```

圖3：證據1 - login[.]us2[.]oraclecloud[.]com目的。圖片來源：CloudSEK

- **證據2 - 真實客戶域名與駭客清單匹配**

駭客提供的樣本資料中，某些網域為Oracle的雲端用戶，並非虛擬或測試用戶。如sbgtv[.]com、nexinfo[.]com、cloudbasesolutions[.]com、nucor-jfe[.]com和rapid4cloud[.]com。

- **證據3 -「login[.]us2[.]oraclecloud[.]com」用於生成SSO設定**

IAM解決方案供應商OneLogin曾經發表有關Oracle Fusion文章，其內容描述如何以SAML作為Oracle Fusion提供SSO進行設定OneLogin，如圖4所示。此外，Oracle Cloud部署和遷移合作夥伴Rainfocus提供的手冊中也建議使用者下載，如圖5所示。

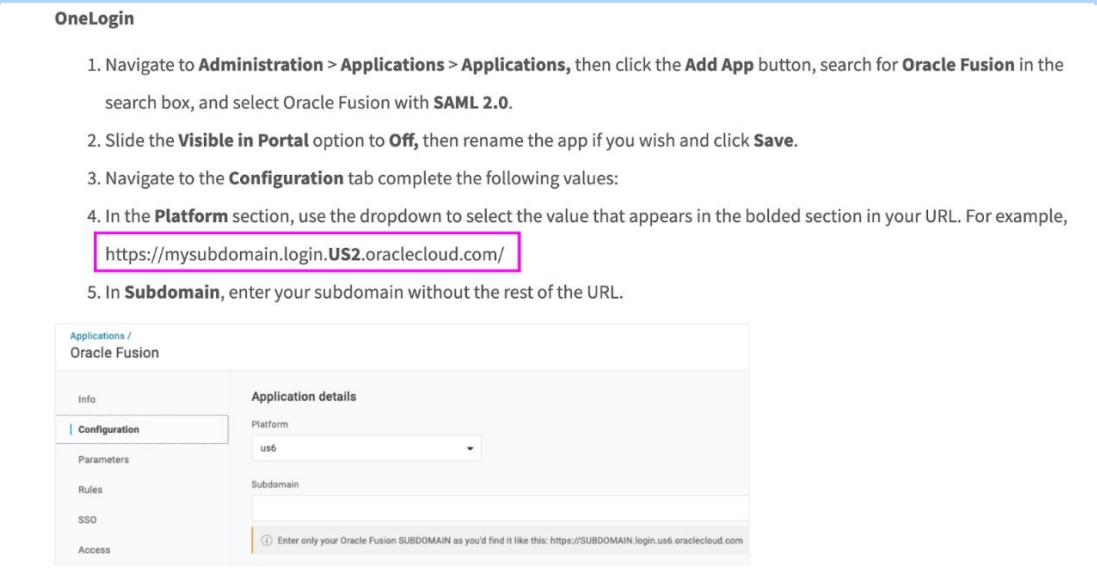


圖4：OneLogin發表的知識庫文章。圖片來源：CloudSEK

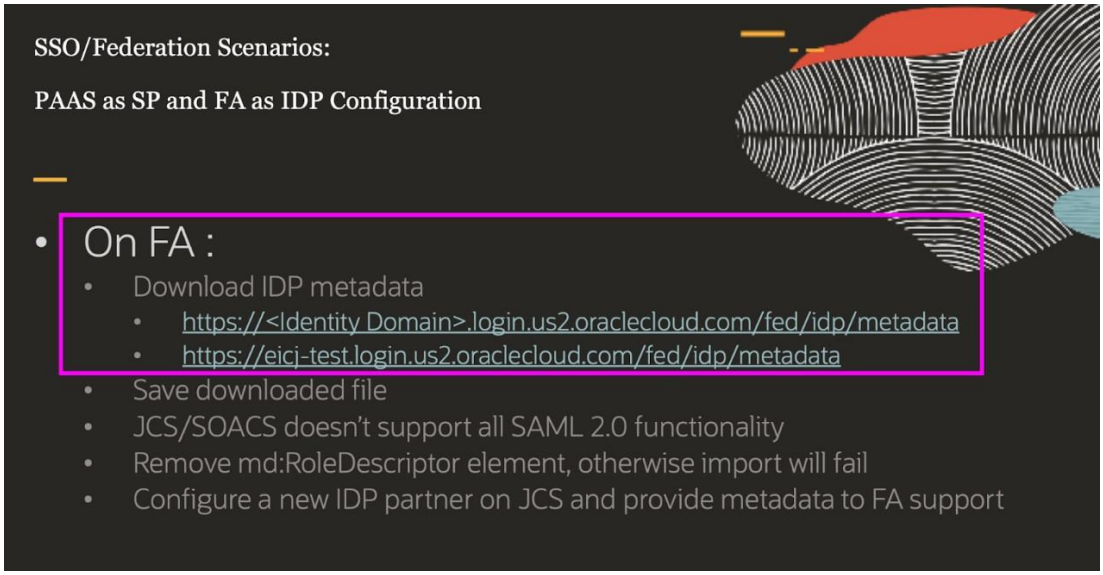


圖5：Rainfocus發布的使用手冊。圖片來源：CloudSEK

本次大規模資料外洩約600萬筆紀錄，其中包括敏感的身分驗證相關資料，增加未授權存取和企業間諜活動的風險。此外，憑證外洩最為嚴重，若加密的SSO和LDAP密碼遭破解，可能導致Oracle雲端環境進一步出現漏洞。同時，駭客可對受影響的企業進行勒索，要求支付贖金將資料刪除。

CloudSEK提出對應措施：

1. 憑證更新：變更所有SSO、LDAP和相關憑證，確保強密碼原則和採用多因子認證(MFA)。
2. 事件調查和取證：進行徹底調查以識別潛在的未經授權的存取並減輕進一步的風險。
3. 威脅情報監控：持續追蹤暗網和駭客在論壇中與洩漏資料相關的討論。

● 相關連結

1. The Biggest Supply Chain Hack Of 2025: 6M Records Exfiltrated from Oracle Cloud affecting over 140k
2. Part 2: Validating the Breach Oracle Cloud Denied – CloudSEK's Follow-Up Analysis
3. Oracle Denies Breach Amid Hacker's Claim of Access to 6 Million Records
4. NVD-CVE-2021-35587

2.3 軟硬體漏洞資訊

2.4.1 Ivanti 旗下設備存在重大資安漏洞，並被積極利用於攻擊活動

CVE 編號	CVE-2025- 22457
影響產品	Ivanti
解決辦法	1. 官方已釋出修補，若有使用以上受影響之產品型號，請參考以下官方網址進行確認：https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US 1. 目前已公告的修補資訊如下： ● Ivanti Connect Secure: 更新 2025/2 發布的 22.7R2.6 安全性修補程式。 ● Pulse Connect Secure 9.1x: 該軟體已終止支援，請聯繫 Ivanti 進行軟體遷移。 ● Ivanti Policy Secure and ZTA Gateways: 安全性修補程式正在開發中，預計於 4/21 與 4/19 發布。 2. 透過官網提供的工具針對系統進行完整性檢查：https://forums.ivanti.com/s/article/KB44755?language=en_US

- 內容說明：

  Ivanti 針對旗下產品 Connect Secure, Pulse Connect Secure(End-of-Support as of 2024/12/31), Policy Secure 及 ZTA Gateways 發布重大資安漏洞公告 (CVE-2025-22457，CVSS 評分 9.0)。該漏洞由緩衝區溢位弱點所造成，允許未經身分驗證的遠端攻擊者可遠端執行任意程式碼 (RCE)，包括執行 Shell 腳本程式與部署惡意程式等，建議用戶儘速採取防護措施，以降低潛在風險，並密切關注官方更新資訊。

- 影響平台：
  - Ivanti Connect Secure 22.7R2.5 及之前的版本
  - Pulse Connect Secure (End-of-Support) 9.1R18.9 及之前的版本
  - Ivanti Policy Secure 22.7R1.3 及之前的版本
  - ZTA Gateways 22.8R2 及之前的版本
- 資料來源：
  1. CVE-2025-22457
  2. CVE-2025-22457
  3. April Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-22457)
  4. Pulse Connect Secure, Ivanti Connect Secure, Policy Secure and Neurons for ZTA Gateways
  5. Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability
  6. Ivanti Releases Security Updates for Connect Secure, Policy Secure & ZTA Gateways Vulnerability
  7. Ivanti Connect Secure (Ics) Integrity Assurance

2.4.2 Fortinet 針對旗下FortiSwitch修補重大資安漏洞

CVE 編號	CVE-2024-48887
影響產品	FortiSwitch
解決辦法	更新至以下版本： FortiSwitch 6.4.15 FortiSwitch 7.0.11 FortiSwitch 7.2.9 FortiSwitch 7.4.5 FortiSwitch 7.6.1

- 內容說明：

  FortiSwitch 是一款由 Fortinet 推出的乙太網路交換器，可與 FortiGate 防火牆整合，實現集中式簡化管理和智慧可擴展性。日前，Fortinet 發布 FortiSwitch GUI 存在重大資安漏洞(CVE-2024-48887，CVSS：9.8)並提出解決方案，此漏洞允許未經身分驗證的遠端攻擊者，透過精心設計的請求修改管理員密碼。

- 影響平台：
  - FortiSwitch 6.4.0 至 6.4.14
  - FortiSwitch 7.0.0 至 7.0.10
  - FortiSwitch 7.2.0 至 7.2.8
  - FortiSwitch 7.4.0 至 7.4.4
  - FortiSwitch 7.6.0
- 資料來源：
  1. Unverified password change via set_password endpoint
  2. CVE-2024-48887

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	 **【費用】** 原價：11,000元/人 軟協會員：8,500元/人 (可單科報名，請洽承辦人) 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。 報名截止： 2025-04-22 **【活動內容 / Event Deails】** 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 **【聯絡窗口】02-2553-3988 分機 816 林專員** **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	 **【費用】** 原價：8,300元/人 早鳥價：7,800元/人(開課前一個月) 軟協會員：7,200元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-05-02 **【活動內容 / Event Deails】** 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 【聯絡窗口】02-2553-3988 分機 816 林專員 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	 【費用】 原價：4,000元/人 早鳥價：3,800元/人(開課前一個月) 軟協會員：3,500元/人 費用含稅、教材及完課證明 報名截止： 2025-05-05 【活動內容 / Event Deails】 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。 **【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】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	 **【費用】** 原價：7,200元/人 早鳥價：6,800元/人(開課前一個月) 軟協會員：6,200元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-05-16 **【活動內容 / Event Deails】** 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** **【聯絡窗口】02-2553-3988 分機 816 林專員** **security@cisanet.org.tw**
【資安院】6/6~7/11醫療資安長高階領導班	
活動時間	**114年6月6日至7月11日，每週1天，上課時間9:00~16:30，合計時數30小時**
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.nics.nat.gov.tw/latest_news/announcements/Event_Information/502e73ec-e39f-4ff1-8b3e-cfb21ae1c584/**
活動概要	 **【主辦單位】** 國家資通安全研究院、台灣醫院協會 **【課程規劃】** 涵蓋資安法規/治理與決策、風險為導向之稽核管控、業務持續運作與資源溝通、系統安全與事件應變及新興科技與安全防護等 5 大主題，以專家講授搭配案例討論、桌上推演實作等教學方式，輔以學員分組討論及專題發表，深化學習效果。 **【招生對象】** 醫療機構與院所之資訊主管、資安主管、資安長(3 年內)或有志發展資安長職涯之資訊或資安領域資深管理或技術人員(建議累計年資 5 年以上)。

	【研習期間】 114 年 6 月 6 日至 7 月 11 日，每週 1 天，上課時間 9:00~16:30，合計時數 30 小時。部分課程(6 月 12 日~7 月 4 日)提供課後線上學習，增加學習彈性，便利學員報名參加。 **【課程費用】** 課程費用原價新臺幣 88,000 元整； 優惠價新臺幣 68,000 元整(5/23 前完成報名及繳費者)； 台灣醫院協會會員優惠價新臺幣 66,000 元整。 **【報名方式】** 1. 資安院官網下載簡章與報名表：https://www.nics.nat.gov.tw/latest_news/announcements/Event_Information/502e73ec-e39f-4ff1-8b3e-cfb21ae1c584/ 2. 採電子郵件(email)通訊報名，以電子郵件(email)方式寄送至本班報名專用電子信箱：nics.tect@nics.nat.gov.tw **【聯絡窗口】** 國家資通安全研究 郭小姐 電話：(02) 2380-0929 電子信箱：nics.tect@nics.nat.gov.tw

【資安學院】6/11-6/12資通系統防護基準實務課程	
活動時間	**2025-06-11 09:00 ~ 2025-06-12 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/5615**

活動概要	 **【費用】** 原價：22,000元/人 早鳥價：20,900元/人(開課前一個月) 軟協會員：請電洽承辦人 費用含稅、教材、餐點及完課證明 報名截止： 2025-06-11 **【活動內容 / Event Deails】** 行政院於 108 年正式實施資通安全管理法，而為了確保資通訊系統之安全，亦於同年 8 月 26 日修正發布附表十之資通系統防護機準，各機關需依系統等級施行「資通系統防護基準」。身為機關資訊管理人員，您更不能忽略該基準之細節，本課程將使您學習如何成為孰悉資通安全防護基準的督導及專責人員，可以勝任該防護基準之督察與落實工作。 **【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】6/13 惡意程式偵測、 分析與防護解析班	
活動時間	**2025-06-13 09:00 ~ 2025-06-13 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/5424
活動概要	 **【費用】** 原價：7,200元/人 早鳥價：6,800元/人(開課前一個月) 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： 2025-06-10 **【活動內容 / Event Deails】** 惡意程式一向為嚴重的資安威脅，從一般的殭屍網路、勒索軟體到精密的 APT 攻擊，惡意程式都扮演重要的攻擊媒介。因此檢測系統中的惡意程式， 為相當重要的資安議題。 本課程將介紹各類型的惡意程式及結構，並從 DEMO 操作了解各種惡意程式的行為特徵，如：Backdoor、rootkit、無檔案攻擊等。了解惡意程式的行為後，課程的另一重點為探討在企業組織內部的基礎 IT 架構中，要如何偵測惡意程式，以及主機感染惡意程式後，如何使用分析工具查找惡意程式進而清除。 **【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】7/3-7/4、7/7-7/9 ISO/IEC 27001:2022 資訊安全管理系統 CQI & IRCA 主導稽核員訓練課程(課程編號：2535)	
活動時間	**2025-07-03 09:00 ~ 2025-07-09 18:30**
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/5429**
活動概要	 **【費用】** 原價：56,000元/人 早鳥價：53,000元/人(開課前兩個月) 軟協會員：請電洽承辦人 費用含稅、教材、餐點及完課證明 報名截止： 2025-06-26 **【活動內容 / Event Deails】** ISO/IEC 27001 是各國企業組織展現資訊安全管理能力的最佳證明，行政院資通安全會報也以此作為對政府單位之資訊安全要求的準則。取得此張證照，不僅肯定個人在資安管理上建置與稽核專業，更展現組織具有資安專業種子人才的能力！ **【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-202504001 / CVE-2025-3361
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： ● iSherlock 4.5與iSherlock 5.5(包含 MailSherlock , SpamSherock, AuditSherlock) 影響套件： ● iSherlock-user-4.5：236(不含)以前版本 ● iSherlock-user-5.5：236(不含)以前版本
問題描述	桓基科技iSherlock之網頁介面存在 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。
解決方法	iSherlock 4.5更新iSherlock-user-4.5套件至236(含)以後版本 iSherlock 5.5更新iSherlock-user-5.5套件至236(含)以後版本
公開日期	2025-04-07
相關連結	**https://www.twcert.org.tw/tw/cp-132-10051-76634-1.html**
桓基科技 iSherlock - OS Command Injection	
TVN / CVE ID	TVN-202504002 / CVE-2025-3362
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： ● iSherlock 4.5與iSherlock 5.5(包含 MailSherlock ,

	SpamSherock, AuditSherlock) 影響套件： ● iSherlock-user-4.5：236(不含)以前版本 ● iSherlock-user-5.5：236(不含)以前版本
問題描述	桓基科技iSherlock之網頁介面存在 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。
解決方法	iSherlock 4.5更新iSherlock-user-4.5套件至236(含)以後版本 iSherlock 5.5更新iSherlock-user-5.5套件至 236(含)以後版本
公開日期	2025-04-07
相關連結	**https://www.twcert.org.tw/tw/cp-132-10053-890b1-1.html**
桓基科技 iSherlock - OS Command Injection	
TVN / CVE ID	TVN-202504003 / CVE-2025-3363
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： ● iSherlock 4.5與iSherlock 5.5(包含 MailSherlock , SpamSherock, AuditSherlock) 影響套件： ● iSherlock-user-4.5：236(不含)以前版本 ● iSherlock-user-5.5：236(不含)以前版本
問題描述	桓基科技iSherlock之網頁介面存在 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。
解決方法	iSherlock 4.5更新iSherlock-user-4.5套件至236(含)以後版本

	iSherlock 5.5更新iSherlock-user-5.5套件至236(含)以後版本
公開日期	2025-04-07
相關連結	https://www.twcert.org.tw/tw/cp-132-10054-84588-1.html
桓基科技 PowerStation - Chroot Escape	
TVN / CVE ID	TVN-202504004 / CVE-2025-3364
CVSS	6.7 (Medium) CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
影響產品	PowerStation 韌體 x64.6.2.213(不含)以前版本
問題描述	桓基科技PowerStation之SSH服務存在Chroot Escape漏洞，已取得root權限之攻擊者可繞過chroot限制存取完整檔案系統。
解決方法	更新韌體至 x64.6.2.213(含)以後版本並重啟PowerStation
公開日期	2025-04-07
相關連結	https://www.twcert.org.tw/tw/cp-132-10057-58c05-1.html
碩網資訊 智能客服 SmartRobot - Server-Side Request Forgery	
TVN / CVE ID	TVN-202504005 / CVE-2025-3572
CVSS	7.5 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
影響產品	SmartRobot v8.0.0(不含)以前版本
問題描述	碩網資訊智能客服SmartRobot存在Server-Side Request Forgery漏洞，允許未經身分鑑別之遠端攻擊者利用此漏洞探測內網資訊，甚至存取任意伺服器本機檔案。
解決方法	聯繫廠商進行修補

公開日期	2025-04-14
相關連結	**https://www.twcert.org.tw/tw/cp-132-10064-6346a-1.html**
一零四資訊科技 eHRMS - Reflected Cross-Site Scripting	
TVN / CVE ID	TVN-202504006 / CVE-2025-3706
CVSS	6.1 (Medium) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
影響產品	eHRMS V202412(含)以前版本
問題描述	一零四資訊科技eHRMS存在Reflected Cross-Site Scripting漏洞，未經身分鑑別之遠端攻擊者可利用釣魚攻擊於使用者端瀏覽器執行任意JavaScript指令。
解決方法	請更新至V202412_Z02(含)以後版本。如需詳細更新說明，請聯繫一零四資訊科技
公開日期	2025-04-28
相關連結	**https://www.twcert.org.tw/tw/cp-132-10079-f0958-1.html**
旭聯科技 eHRD CTMS	
TVN / CVE ID	TVN-202504007 / CVE-2025-3707
CVSS	7.5(High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
影響產品	eHRD CTMS 10.13(含)以前版本
問題描述	旭聯科技eHRD CTMS存在SQL Injection漏洞，允許已取得一般權限之遠端攻擊者注入任意SQL指令以讀取資料庫內容。
解決方法	聯繫廠商取得修補程式
公開日期	2025-04-30
相關連結	**https://www.twcert.org.tw/tw/cp-132-10083-4ed7f-1.html**

樂衍有限公司樂易秀醫事管理系統 - SQL Injection	
TVN / CVE ID	TVN-202504008 / CVE-2025-3708
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	樂易秀醫事管理系統 V3.0.25(含)以前版本
問題描述	樂衍有限公司樂易秀醫事管理系統存在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	更新至 V3.0.30(含)以後版本
公開日期	2025-04-30
相關連結	**https://www.twcert.org.tw/tw/cp-132-10085-69e16-1.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4月30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/**