TWCERT/CC 資安情資電子報

2024 年 11 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

2024台灣資安通報應變年會：預見資安威脅 賦能通報聯防

為了協助資通安全管理法納管對象以外的民間企業提升資安防護能力，數位發展部已責成國家資通安全研究院，自2024年1月起接手營運台灣電腦網路危機處理暨協調中心（TWCERT/CC）。該中心將提供全年24小時不間斷的資安事件通報、情資分享、應變協調、國際合作及意識提升等多項企業資安服務，旨在強化台灣整體的資安防護網。

TWCERT/CC主辦的第八屆台灣資安通報應變年會將於11月22日盛大舉行，主題為「預見資安威脅 賦能通報聯防」。此次年會將邀集國內各資安事件協處單位、企業代表及學術界專家，共同分享年度資安成果與最新趨勢。與會者將有機會深入探討以下重要議題：

- 資安聯防最佳實踐：分享各界在面對資安威脅時的成功經驗與策略。
- 資安威脅趨勢發展：分析當前及未來的資安威脅，幫助企

業預見潛在風險。

- 實務經驗分享：邀請業界專家分享實際案例，提供參與者具體的應對建議。

TWCER/CC期望在本次年會提升企業人員的資安意識，並強化台灣企業在面對各類資安挑戰時的韌性。

本年會將開放實體與線上參與，為確保座位有限，實體參加者將優先開放予聯盟會員。

專業人士可透過以下連結報名參加：https://activity.twcert.org.tw/。歡迎各界專業人士踴躍報名，共同參與這場提升資安意識的重要盛會。

隨著數位化進程的加速，企業面臨的資安威脅日益嚴峻。透過此次年會，我們希望能夠促進各界對於資安議題的關注與合作，共同打造更安全的數位環境。

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 新型惡意軟體SteelFox偽裝破解工具竊取使用者敏感資料

SteelFox是一款新型的惡意軟體，主要透過論壇貼文、Torrent追蹤器與部落格等平台進行傳播。該惡意軟體偽裝成知名流行軟體的破解工具，包括Foxit PDF Editor、AutoCAD和JetBrains等，旨在竊取使用者的信用卡資料、瀏覽紀錄及其他敏感資料，甚至利用使用者的設備進行加密貨幣挖礦。

卡巴斯基的研究人員指出，SteelFox並不針對個人或組織，而是對全球無差別進行大規模攻擊，目前資安產品成功檢測並阻止超過11,000次的攻擊，受害者主要分布位於巴西、中國、俄羅斯、墨西哥等國家。該惡意軟體最初透過論壇或Torrent追蹤器上散布含有惡意軟體的破解工具下載連結，誘導使用者下載安裝。當使用者啟動破解工具時，SteelFox安裝過程要求授予管理者權限，並在系統中植入惡意程式，以便進一步發起後續攻擊。

圖1：SteelFox利用論壇進行傳播。圖片來源：SECURELIST

SteelFox使用AES-128加密技術避開嵌入式PE解析器進行偵測，隨後採用AES-NI指令集簡化加密過程。接著建立新的系統服務，使其能透過重新啟動，讓惡意程式在系統中保持運作狀態。當SteelFox成功控制受害者主機，會進一步在系統檔案中植入更多惡意軟體，且將自己註冊為Windows服務，使得檢測和刪除惡意檔案變得更加困難。

當取得管理者權限後，將會創建在內部運行的WinRing0.sys服務，此驅動程式存在CVE-2020-14979 與CVE-2021-41285 等漏洞，攻擊者可利用前述漏洞將權限提升至NT/SYSTEM等級，NT/SYSTEM權限比管理員權限更強大，允許攻擊者不受限制存取訪問系統任何資源，此驅動程式也是XMRig加密貨幣挖礦的一部分，使得攻擊者能夠使用受害者設備進行加密貨幣挖礦。

此外，SteelFox設計複雜的自我驗證機制，以確保只在合法的服務環境中執行，以避免被防毒軟體檢測。

SteelFox顯著的特點是安全通訊模型，一旦嵌入系統，惡意軟體自動透過動態分配IP位置和C2伺服器進行加密通訊，此連線採用SSL pinning 和 TLS v1.3，有效防止數據在傳輸過程中被攔截。當連

線建立後，攻擊者開始收集受害者的敏感資料，如cookie、信用卡資料和瀏覽紀錄等，並將這些資料組合成JSON格式後發送至C2伺服器。

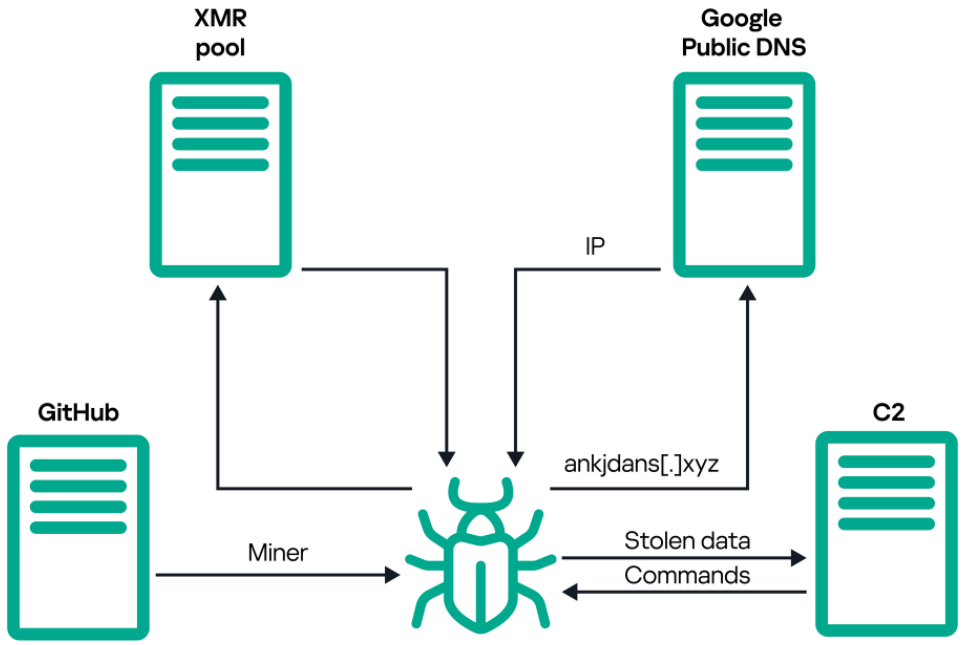


圖2：SteelFox的連接圖。圖片來源：SECURELIST

為了降低此類惡意活動，建議使用者從官方網站下載正版軟體，並對於任何免費破解軟體保持高度警惕。避免下載來路不明的軟體或破解工具，並定期更新作業系統及防毒軟體，以提高應對各類惡意程式的防範能力。

- 資料來源：
  1. New SteelFox Trojan mimics software activators, stealing sensitive data and mining cryptocurrency
  2. New SteelFox malware hijacks Windows PCs using vulnerable driver
  3. SteelFox Trojan spreads via forums disguised as Foxit, AutoCad

2.2 資安趨勢

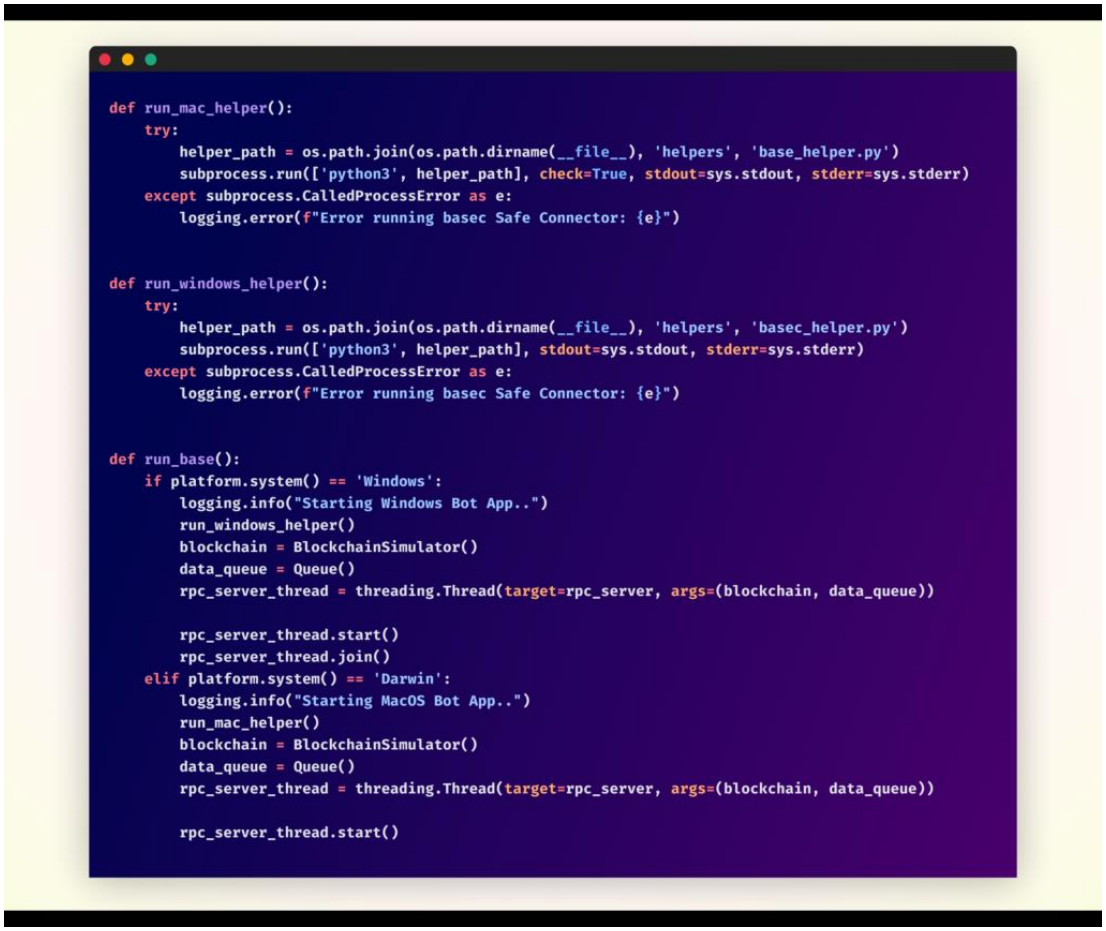
2.2.1 CryptoAITools：針對加密錢包的惡意軟體

Checkmarx安全研究團隊近期發現一個名為CryptoAITools新的惡意Python套件，這個套件偽裝成加密貨幣交易工具，但實際上具備竊取敏感資料與受害者加密錢包資產的功能。CryptoAITools透過Python Package Index (PyPI)和GitHub儲存庫進行擴散，此套件從PyPI下架之前，已經累積下載超過1300次。

Checkmarx安全研究團隊針對CryptoAITools的主要特點和發現包含：

- 該惡意軟體採用多種社交工程策略進行散播，包括在PyPI上最初的惡意軟體套件「cryptoaitools」、偽造的Github儲存庫則是名為「Meme-Token-Hunter-Bot」、模仿合法的加密貨幣交易機器人的虛假網站(coinsw[.]app)、透過Telegram與受害者互動。

- 使用者安裝惡意軟體後，CryptoAITools利用套件中的「__init__.py」檔，可確認目標是Windows或macOS作業系統，以執行相應版本的惡意軟體。



```
def run_mac_helper():
    try:
        helper_path = os.path.join(os.path.dirname(__file__), 'helpers', 'base_helper.py')
        subprocess.run(['python3', helper_path], check=True, stdout=sys.stdout, stderr=sys.stderr)
    except subprocess.CalledProcessError as e:
        logging.error(f"Error running basec Safe Connector: {e}")


def run_windows_helper():
    try:
        helper_path = os.path.join(os.path.dirname(__file__), 'helpers', 'basec_helper.py')
        subprocess.run(['python3', helper_path], stdout=sys.stdout, stderr=sys.stderr)
    except subprocess.CalledProcessError as e:
        logging.error(f"Error running basec Safe Connector: {e}")


def run_base():
    if platform.system() == 'Windows':
        logging.info("Starting Windows Bot App..")
        run_windows_helper()
        blockchain = BlockchainSimulator()
        data_queue = Queue()
        rpc_server_thread = threading.Thread(target=rpc_server, args=(blockchain, data_queue))

        rpc_server_thread.start()
        rpc_server_thread.join()
    elif platform.system() == 'Darwin':
        logging.info("Starting MacOS Bot App..")
        run_mac_helper()
        blockchain = BlockchainSimulator()
        data_queue = Queue()
        rpc_server_thread = threading.Thread(target=rpc_server, args=(blockchain, data_queue))

        rpc_server_thread.start()
```

圖3 CryptoAITools辨別受害者的作業系統，圖片來源於Checkmarx

CryptoAITools將圖形使用者介面(GUI)作為社交工程策略的一部分，旨在分散受害者的注意力，同時收集有關加密貨幣的敏感資訊，包含錢包資料、瀏覽器資料及敏感系統檔案等。

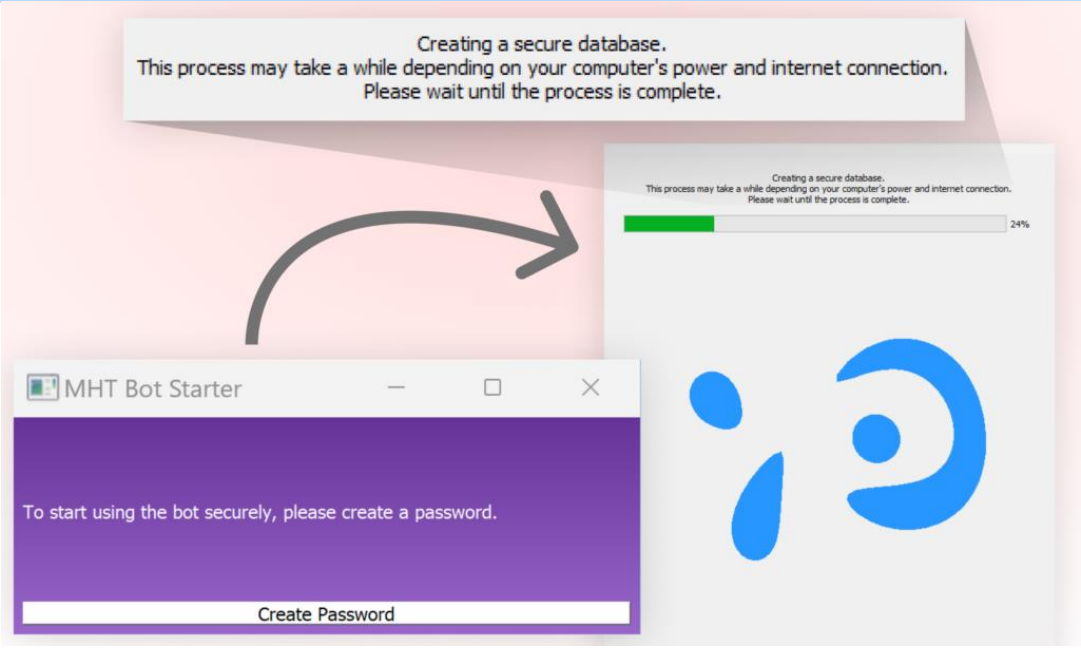


圖4 CryptoAITools的使用者介面，圖片來源於Checkmarx

該套件初始感染階段，透過腳本從虛假網站下載其他惡意元件，執行額外的有效負載，從而啟動多階段感染過程。惡意軟體精心設計具有說服力的加密貨幣交易機器人服務網站，搭配虛假用戶評論和訂閱者數量，試圖增加可信度。

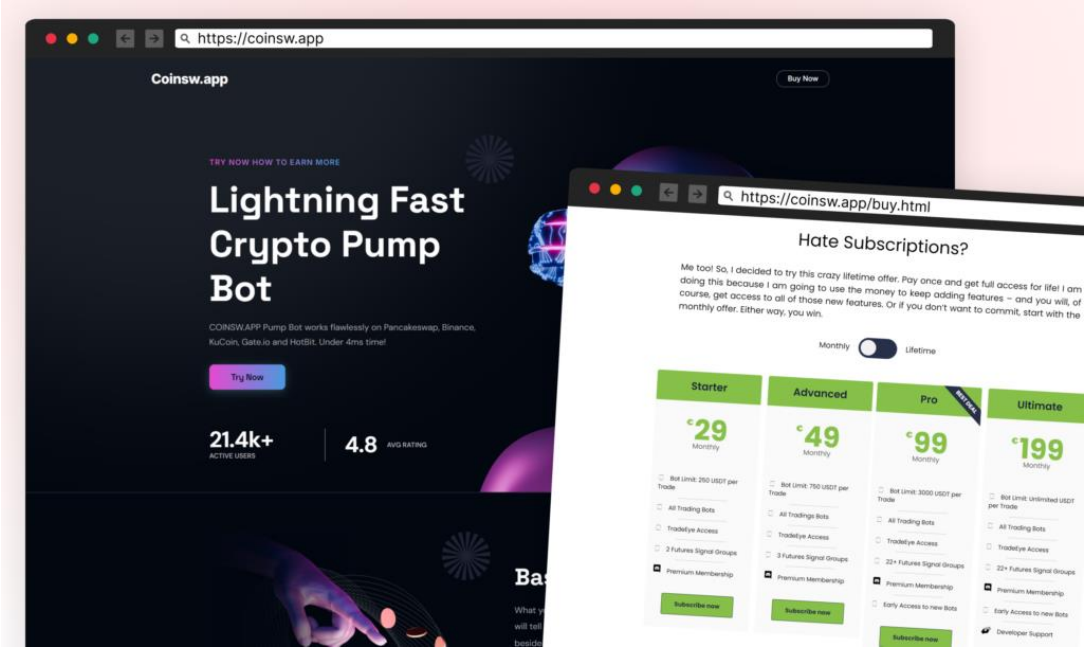


圖5 CryptoAITools的虛假網站，圖片來源於Checkmarx

呼籲使用者在下載和安裝任何第三方套件時特別小心，應仔細檢查來源以及可信度，建議使用官方渠道，同時定期更新安全軟體，強化防護措施。

- 資料來源：
  1. Researchers Uncover Python Package Targeting Crypto Wallets with Malicious Code
  2. Cryptocurrency Enthusiasts Targeted in Multi-Vector Supply Chain Attack

2.3 資安小知識

2.3.1 新型身分驗證方式PassKey

隨著數位安全威脅日益增加，傳統的密碼系統面臨越來越大安全挑戰。為了應對這些威脅，一種名為「PassKey」的新技術應運而生。PassKey是基於FIDO2和Web Authentication標準發展而來，已被主流平台和瀏覽器廣泛支持，是一種新型的身份驗證方式，旨在取代傳統密碼，提高安全性和使用便利性。

PassKey採用公私鑰加密技術作為一種全新認證方式，不僅能顯著提高使用者帳戶安全性，亦可改善使用者的登入體驗。當使用者在支援PassKey的網站或應用程式註冊時，系統會生成一對密鑰。

- 公開密鑰(Public Key)：儲存於伺服器，用於身份驗證，但無法被用來假冒用戶身份。
- 私密密鑰(Private Key)：儲存於用戶的設備，僅限用戶可透過設備的私鑰生成數位簽章，而簽章主要用於與公鑰進行驗證。

在登入過程中，使用者可以透過生物識別(如指紋、臉部辨識)或本地端的PIN碼進行解鎖設備，完成登入操作，簡化傳統密碼帶來的繁瑣。

透過採用PassKey技術，使用者可以享受安全且便捷的登入體驗，有效保護數位身份。此外，建議定期更新軟體和瀏覽器至最新版本，確保系統始終處於最新狀態，從而最大程度提升安全性。

2.3.2 數位時代如何識別假新聞

在數位時代，假新聞的傳播速度極快，不僅影響公眾輿論，還可能對個人與組織的資安造成威脅。透過加強自身的識別能力和謹慎行為，才能有效減少假新聞對個人及社會的潛在危害，以下是一些辨識假新聞的技巧：

1. 假新聞往往具有誇張的標題、缺乏可靠的來源引用，且資訊模糊不清。
2. 分享或相信某條新聞前，務必查證其來源，並比對前後文，避免斷章取義。倘若報導來自不熟悉的機關/組織，可以查詢其他可靠的資料來源驗證該信息。
3. 假新聞有時會被用來誘騙用戶提供個人信息，因此不要隨意點擊可疑連結或提供在不明網站上提供敏感資訊。
4. 使用社交媒體時，應該保持懷疑態度，特別對於不明帳號或廣為流傳的消息要特別小心。
5. 消除個人成見，以中立的態度看待消息，並只分享可信的新聞。
6. 善用各種假訊息查證管道來核實可疑新聞，例如台灣事實查核

中心(https://tfc-taiwan.org.tw/)。

面對數位時代的假新聞挑戰，提升識別能力和謹慎行為是關鍵。透過注意標題和來源、查證信息、保持警覺以及以中立態度處理消息，能有效減少假新聞對個人和社會的潛在危害。

2.3.3 防範加密貨幣地址中毒攻擊

地址中毒(address poisoning)是近年來常被駭客利用的一種精巧網路釣魚手法，該攻擊主要發生在數據透明且公開的區塊鏈上，若受害者在操作加密貨幣交易的過程中，沒有仔細逐字檢查交易帳戶地址，便會掉落攻擊者所設計的圈套中，可能造成巨大財產損失。

地址中毒之攻擊手法十分精巧，利用的是人的「習慣」，首先，攻擊者針對經常在個人多個帳戶之間進行資金轉移，或是規律向某帳號發送資金的帳戶進行監控，攻擊者可透過帳號生成器建立相似的假地址，並向受害者發送一筆交易，使得假地址被記錄到受害者的交易紀錄中，當受害者進行交易時，可能被誘導將加密貨幣轉移至攻擊者的假地址。

呼籲加密貨幣的使用者在進行貨幣交易時，避免直接從歷史交易中複製地址，並請務必逐字確認交易地址是否正確。

2.4 軟硬體漏洞資訊

2.4.1 Fortinet多項產品存在安全漏洞(CVE-2024-23113)

CVE 編號	CVE-2024-23113
影響產品	Fortinet
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明，網址如下： https://www.fortiguard.com/psirt/FG-IR-24-029

- 內容說明：

  近期研究人員發現 Fortinet 多項產品存在格式化字串(Format String)漏洞(CVE-2024-23113)，未經身分鑑別之遠端攻擊者可利用特製封包於受影響產品執行任意程式碼。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - FortiOS 7.0.0 至 7.0.13、7.2.0 至 7.2.6 及 7.4.0 至 7.4.2 版本
  - FortiProxy 7.0.0 至 7.0.14、7.2.0 至 7.2.8 及 7.4.0 至 7.4.2 版本
  - FortiPAM 1.0.0 至 1.0.3、1.1.0 至 1.1.2 及 1.2.0 版本
  - FortiSwitchManager 7.0.0 至 7.0.3 與 7.2.0 至 7.2.3 版本
- 資料來源：

  1. https://nvd.nist.gov/vuln/detail/CVE-2024-23113
  2. https://www.fortiguard.com/psirt/FG-IR-24-029
  3. https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=11314
  4. https://www.ithome.com.tw/news/165432

2.4.2 葳橋資訊行政管理資訊系統存在安全漏洞

CVE 編號	CVE-2024-10200、CVE-2024-10201 及 CVE-2024-10202
影響產品	葳橋資訊行政管理資訊系統
解決辦法	官方已針對漏洞釋出修復更新，請聯繫廠商進行修補。

- 內容說明：

  近期研究人員發現橋資訊行政管理資訊系統存在數個安全漏洞(CVE-2024-10200、CVE-2024-10201 及 CVE-2024-10202)，針對 CVE-2024-10200，攻擊者在不需身分鑑別的情況下可讀取任意系統檔案；而針對 CVE-2024-10201 與 CVE-2024-10202，攻擊者在取得一般權限後，可遠端執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - 葳橋資訊行政管理資訊系統
- 資料來源：

1. https://www.twcert.org.tw/tw/cp-132-8159-0f7a2-1.html
2. https://www.twcert.org.tw/tw/cp-132-8160-756b6-1.html
3. https://www.twcert.org.tw/tw/cp-132-8162-dc491-1.html
4. https://nvd.nist.gov/vuln/detail/CVE-2024-10200
5. https://nvd.nist.gov/vuln/detail/CVE-2024-10201
6. https://nvd.nist.gov/vuln/detail/CVE-2024-10202

第 3 章、資安研討會及活動

- **資安研討會**

【資安院】11/2~3、11/9~10資安菁英實戰培育課程 第3期臺北場(四日)	
活動時間	2024/11/2、3、9、10
活動地點	臺北創新實驗室-會議A廳（臺北市內湖區洲子街12號2樓（近捷運港墘站2號出口））
活動網站	https://nicste2.kktix.cc/events/113elitecourse3
活動概要	 **【費用】** 免費 報名截止： 2024-10-17 **【活動內容 / Event Deails】** 菁英班課程舉辦到今年已經第 4 年了！透過國際級講師傳授資安秘技與實作，獲得一片好評，今年更增添了更多演練與實作內容，讓大家不侷限於紙上談兵，而是將所學技術與理論實際操作應用，可以把課程所學正式內化成自己的能力！ 不論您是在一般企業、政府單位、資安公司或是其他單位的在職資安技術/研發人員，都歡迎踴躍報名！此次活動將由政府全額補助，所以名額有限，千萬要把握機會喔～

《第 3 期臺北場課程資訊》	
113 年 11 月 2 日至 3 日 (週六、週日)	藍隊解壓縮 - 從零開始建構企業防禦工事：鄭仲倫講師
113 年 11 月 9 日(週六)	雲端保衛戰：藍隊的雲端安全生存指南：林殿智講師
113 年 11 月 10 日 (週日)	網路威脅防禦競賽

【主辦單位】國家資通安全研究院

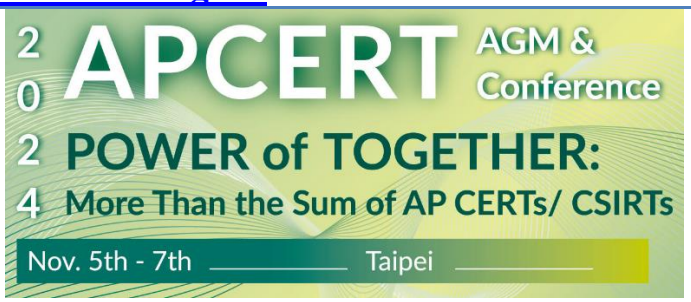
【指導單位】數位發展部資通安全署

【執行單位】社團法人台灣駭客協會

【聯絡窗口】02-2380-0923 鄭規劃師

mailto:te-atc@nics.nat.gov.tw

【TWCERT/CC】APCERT資安年會

活動時間	**2024/11/5~7**
活動地點	**台北萬豪酒店(台北市中山區樂群二路199號)**
活動網站	**https://apcert2024con.org.tw/**
活動概要	 **【費用】** 免費 報名截止： 2024-10-30 **【活動內容 / Event Deails】**

	亞太區電腦事件協調組織(APCERT)將於2024年11月5日至7日在台北萬豪酒店舉辦年度重要活動—「APCERT 2024會員年會暨國際資安研討會」。此次年會由台灣電腦網路危機處理暨協調中心(TWCERT/CC)主辦，主題為「Power of Together: More Than the Sum of AP CERTs/CSIRTs」。 本屆年會將分為兩部分：11月5日至6日為APCERT會員年會及閉門會議，11月7日則與全球最大的資安應變與安全組織Forum for Incident Response and Security Teams共同舉辦公開研討會。該公開研討會將針對多個資安主題進行深入探討，包括資安威脅趨勢、威脅情報與分析、新興技術、治理與管理，以及協作模式等。此次活動旨在促進亞太地區資安專家的交流，並增強各成員間的合作能力，以更有效地應對日益嚴峻的網路安全威脅。APCERT自2003年成立以來，一直致力於建立亞太地區資安專家互信社群，並在面對重大資安事件時提供跨國協作應變的支持。 歡迎各界專業人士參加，共同分享最新的資安洞見與技術經驗，攜手提升整體的資安防護能力。 **【主辦單位】**亞太區電腦事件協調組織（APCERT）、台灣電腦網路危機處理暨協調中心（TWCERT/CC）
【資策會】11/22 CyberDay 2024資安產業日	
活動時間	**2024/11/22**
活動地點	**臺北創新實驗室-會議A廳（臺北市內湖區洲子街12號2樓（近捷運港墘站2號出口））**
活動網站	**https://www.cyberday.com.tw/**

活動概要	 **【費用】** 免費 報名截止： 2024/11/22 **【議程時間】**113 年 11 月 22 日(五) 10:00-16:00 **【議程地點】**臺南沙崙資安暨智慧科技研發大樓 **【議程目標】** 數位發展部數位產業署致力於推動臺灣產業數位轉型及發展數位經濟，協助產業因應數位挑戰提升資安韌性並強化產業資安防護，特於 113 年 11 月 22 日(五)假臺南沙崙資安暨智慧科技研發大樓，舉辦

	數產署資安年度盛會【CyberDay 2024 資安產業日】，藉以展示本署在資安產業、產業資安、資安人培、資安研發執行成果，並期許成為資安供給方、資安需求方的交流媒合平台，持續與資安的產、官、學各界共同合作，推動臺灣資安產業進一步發展。 **【活動議程】** ● 開幕式暨主題演講，分享資安新趨勢 ● 產業資安研討聚焦供應鏈聯防，以實戰經驗探討其技術應用 ● 資安業者攤位展示，提供資安解決方案與創新技術 ● 後量子 PQC 遷移高峰會暨創新應用推廣說明會聚焦加密技術的應用與遷移策略 ● 以資安遊戲寓教於樂帶動認識資安議題 ● 資安新秀快講展現產學合作成果，分享專題實作歷程 **【主辦單位】數位發展部數位產業署** **【指導單位】數位發展部**

● **TWCERT/CC 資安活動紀事**

APCERT 2024會員年會暨國際資安研討會於台北盛大舉行，台灣強化亞太地區資安協作	
活動時間	**113.11.5~6**
活動概要	亞太區電腦事件協調組織(APCERT)及台灣電腦網路危機處理暨協調中心(TWCERT/CC)共同主辦APCERT2024會員年會暨國際資安研討會，於11月5日至6日在台北萬豪酒店舉行，並於7日接續與全球規模最大之資安應變與安全組織Forum for Incident Response and Security Teams (FIRST)共同辦理亞太地區資安研討會 (APCERT& FIRST Regional Symposium for Asia Pacific)。兩大國際盛會匯集來自亞太及全球約25個經濟體與國內的資安專家，齊聚一堂針對全球資

安威脅趨勢、AI新興科技應用對資安的威脅及機會、資安治理強化、國際合作協防及資安人才培訓等重大議題，共同探討並提出因應對策。

蕭美琴副總統親臨會場致詞時特別提及，隨著全球數位化的快速推進，資安威脅日益增加，唯有透過全球合作、情報分享以及技術協作，才能有效應對這項嚴峻的挑戰。蕭副總統強調，台灣將資安視為非常重要的政府工作，事實上，資安是最優先的項目，是在面臨自然災害或其他威脅下，政府服務能持續運作以及人民經濟活動能正常進行的基礎。此次會議將有助於進一步加強亞太地區各資安機構間的合作，推動資安技術的創新，並提升我國的資安能力。蕭副總統特別感謝共同主辦單位 FIRST，擴大此次研討會的國際影響力。此外，本次 FIRST 特別贊助來自亞太地區的女性資安專家出席會議，鼓勵更多女性參與資安領域，也讓我們的國際資安合作更加多元。

本次會議承辦單位TWCERT/CC在今年一月起，由行政法人國家資通安全研究院接手運營。數發部次長闕河鳴表示，透過TWCERT/CC這個平台，台灣正進一步深化與亞太及全球資安組織的鏈結及合作，共同攜手維護網路世界民主自由。

FIRST 董事會代表(Board of Directors) 內田有香子(Yukako Uchida)感謝TWCERT/CC為亞太地區研討會重回實體形式所作的努力。她表示本次會議展現FIRST與台灣及亞太區域合作夥伴的緊密合作及信任關係，期盼未來FIRST能持續在亞太地區擴大推動並強化資安事件應變社群的鏈結。

本屆年會是APCERT會員相隔四年後久違的實體會議，也是台灣繼2014年，再度主辦APCERT國際年會。今年年會以「Power of Together: More Than the Sum of APCERTs/CSIRTs」為主題，會議針對當前全球面臨的資安挑戰、AI等新興科技的應用對資安的威脅與機會、資安治理強化、跨國合作聯防、人才培訓及未來發展策略、

	區域資安協作的推動等議題進行探討，期盼匯聚各國力量，共同提升資安韌性，以應對全球日益嚴峻的網路威脅。台積電、奧義智慧與趨勢科技等台灣企業亦指派專家出席，並分享台灣的資安防護及治理經驗，展現國內業界對全球公私協力共同防護資安的積極參與。    
資安院攜手產業提升資安韌性，跨域協作聯防成就資安共好	
活動時間	**113.11.22**
活動概要	國家資通安全研究院於11月22日辦理台灣電腦網路危機處理暨協調中心(TWCERT/CC)「2024台灣資安通報應變年會」。為應對全球複雜多變的資安威脅與風險，2024年會以「預見資安威脅，賦能通報聯防」為主題，邀集來自數位發展部、資安院、台積電、鴻海、華碩、合勤、雲林科大、永豐銀行、奧義智慧科技等公私部門的專家齊聚一堂，共同探討當前的重大資安議題、分享有效應對資安事件的實務經驗，以及如何強化跨域協作聯防提升企業的整體防護能力。

數位發展部闕河鳴政務次長於年會致詞表示，2024年國際間發生許多影響重大的資安事件，攻擊者的手法不斷推陳出新，而且越來越隱蔽，不易及時發覺，並且攻擊規模與影響範圍也日益擴大。面對日愈嚴峻的資安威脅，單一的政府機關、企業或組織已無法獨自有效的及時因應，有賴政府與民間企業共同攜手協作聯防，並且重新思考及強化整體資安防護架構與應對策略。

資安院配合數發部強化企業資安防護政策，自今年1月1日起接手營運TWCERT/CC，提供產業全年24小時不間斷的資安事件通報、情資分享、應變協調、國際合作、意識提升等資安服務。資安院接手營運TWCERT/CC之後，透過各種管道持續擴大與民間企業及公協會合作，進一步強化產業整體資安防護量能。

資安院何全德院長於會中表示，因應資安威脅日趨複雜與影響範圍擴大，資安問題已不再是單一國家、單一企業或組織可以獨自有效解決，亟需仰賴跨國、跨領域、跨組織的資安協作與聯防來共同防護數位網路安全。企業需具備及持續提升應對資安事件的基本能力，建立即時的事件通報與聯防協處機制並且定期演練，才能有效因應錯綜複雜的資安威脅與挑戰。

本次年會特別安排華碩金慶柏資安長、資安院通報應變中心孫偉哲主任、永豐銀行高大宇副總經理、奧義智慧邱銘彰創辦人、雲林科大林峻立教授、台積電資訊安全處許映威處長、合勤投控游政卿資安長、鴻海李維斌資安長等資安專家，發表專題演講，針對數位時代的全球資安治理、TWCERT/CC成果與願景、資安事件實戰應對、生成式AI影響下之資安新戰略、零信任架構實戰經驗及企業供應鏈數位安全等議題，進行趨勢探討分析與經驗分享。蕭美琴副總統親臨會場致詞時特別提及，隨著全球數位化的快速推進，資安威脅日益增加，唯有透過全球合作、情報分享以及技術協作，才能有效應對這項嚴峻的挑戰。蕭副總統強調，台灣將資安視為非常重要的政府工作，事實上，資安是最優先的項目，是在面臨自然災害

或其他威脅下，政府服務能持續運作以及人民經濟活動能正常進行的基礎。此次會議將有助於進一步加強亞太地區各資安機構間的合作，推動資安技術的創新，並提升我國的資安能力。蕭副總統特別感謝共同主辦單位 FIRST，擴大此次研討會的國際影響力。此外，本次 FIRST 特別贊助來自亞太地區的女性資安專家出席會議，鼓勵更多女性參與資安領域，也讓我們的國際資安合作更加多元。

本次會議承辦單位TWCERT/CC在今年一月起，由行政法人國家資通安全研究院接手運營。數發部次長闕河鳴表示，透過TWCERT/CC這個平台，台灣正進一步深化與亞太及全球資安組織的鏈結及合作，共同攜手維護網路世界民主自由。

FIRST 董事會代表(Board of Directors) 內田有香子(Yukako Uchida)感謝TWCERT/CC為亞太地區研討會重回實體形式所作的努力。她表示本次會議展現FIRST與台灣及亞太區域合作夥伴的緊密合作及信任關係，期盼未來FIRST能持續在亞太地區擴大推動並強化資安事件應變社群的鏈結。

本屆年會是APCERT會員相隔四年後久違的實體會議，也是台灣繼2014年，再度主辦APCERT國際年會。今年年會以「Power of Together: More Than the Sum of APCERTs/CSIRTs」為主題，會議針對當前全球面臨的資安挑戰、AI等新興科技的應用對資安的威脅與機會、資安治理強化、跨國合作聯防、人才培訓及未來發展策略、區域資安協作的推動等議題進行探討，期盼匯聚各國力量，共同提升資安韌性，以應對全球日益嚴峻的網路威脅。台積電、奧義智慧與趨勢科技等台灣企業亦指派專家出席，並分享台灣的資安防護及治理經驗，展現國內業界對全球公私協力共同防護資安的積極參與。


2024台灣資安通報應變年會
預見資安威脅 賦能通報聯防


2024台灣資安通報應變年會
預見資安威脅 賦能通報聯防

第 4 章、TVN 漏洞公告

TWCERT/CC 本月份發布之CVSS 3分數為8.8以上之漏洞資訊如下表：

欣學英資訊 Webopac - SQL Injection	
TVN / CVE ID	TVN-202411001 / CVE-2024-11016
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	Webopac 6, Webopac 7
問題描述	Webopac 6, Webopac 7
解決方法	更新Webopac 6 至 6.5.1(含)以後版本 更新Webopac 7 至 7.2.3(含)以後版本
公開日期	2024-11-08
相關連結	**https://www.twcert.org.tw/tw/cp-132-8209-bf75d-1.html**

欣學英資訊 Webopac - Arbitrary File Upload	
TVN / CVE ID	TVN-202411002 / CVE-2024-11017
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	Webopac 6, Webopac 7
問題描述	欣學英資訊 Webopac 未妥善驗證上傳檔案類型，允許已取得一般權限之遠端攻擊者上傳網頁後門程式並執行，進而於伺服器上執行任意程式碼。
解決方法	更新 OAKlouds-webbase-2.0 至 1162(含)以後版本 更新 OAKlouds-webbase-3.0 至 1162(含)以後版本
公開日期	2024-10-14

相關連結	**https://www.twcert.org.tw/tw/cp-132-8130-89bb1-1.html**

欣學英資訊 Webopac - Arbitrary File Upload	
TVN / CVE ID	TVN-202411002 / CVE-2024-11017
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	Webopac 6, Webopac 7
問題描述	欣學英資訊 Webopac 未妥善驗證上傳檔案類型，允許已取得一般權限之遠端攻擊者上傳網頁後門程式並執行，進而於伺服器上執行任意程式碼。
解決方法	欣學英資訊 Webopac 未妥善驗證上傳檔案類型，允許已取得一般權限之遠端攻擊者上傳網頁後門程式並執行，進而於伺服器上執行任意程式碼。
公開日期	2024-11-08
相關連結	**https://www.twcert.org.tw/tw/cp-132-8211-a2da2-1.html**

欣學英資訊 Webopac - Arbitrary File Upload	
TVN / CVE ID	TVN-202411003 / CVE-2024-11018
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	Webopac 6, Webopac 7
問題描述	欣學英資訊 Webopac 未妥善驗證上傳檔案類型，允許未經身分鑑別之遠端攻擊者上傳網頁後門程式並執行，進而於伺服器上執行任意程式碼。

解決方法	更新Webopac 6 至 6.5.1(含)以後版本 更新Webopac 7 至 7.2.3(含)以後版本
公開日期	2024-11-08
相關連結	https://www.twcert.org.tw/newepaper/cp-151-8213-3413b-3.html

欣學英資訊 Webopac - SQL Injection	
TVN / CVE ID	TVN-202411005 / CVE-2024-11020
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	Webopac 6, Webopac 7
問題描述	欣學英資訊 Webopac 存在 SQL Injection 漏洞，未經身分鑑別之遠端攻擊者可於特定參數注入任意SQL指令讀取、修改及刪除資料庫內容。
解決方法	更新Webopac 6 至 6.5.1(含)以後版本 更新Webopac 7 至 7.2.3(含)以後版本
公開日期	2024-11-08
相關連結	https://www.twcert.org.tw/tw/cp-132-8217-05b42-1.html

D-Link DSL6740C - Incorrect Use of Privileged APIs	
TVN / CVE ID	TVN-202411013 / CVE-2024-11068
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	DSL6740C
問題描述	D-Link 數據機 DSL6740C 存在Incorrect Use of Privileged APIs漏洞，未經身分鑑別之遠端攻擊者可透過特定API修

	改任意使用者密碼後以該使用者登入Web、SSH及Telnet等服務。
解決方法	受影響設備已不再支援更新，建議汰換設備
公開日期	2024-11-11
相關連結	https://www.twcert.org.tw/tw/cp-132-8227-f3f3b-1.html

GeoVision 已停止維護之設備 - OS Command Injection	
TVN / CVE ID	TVN-202411014 / CVE-2024-11120
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	GV-VS12,GV-VS11,GV-DSP_LPR_V3,GVLX 4 V2,GVLX 4 V3
問題描述	GeoVision部分已停止支援設備存在OS Command Injection漏洞，未經身分鑑別之遠端攻擊者可利用此漏洞注入系統指令並於設備上執行。另外，我們已收到相關報告顯示該漏洞已遭利用。
解決方法	該產品已不再維護，建議汰換設備
公開日期	2024-11-15
相關連結	https://www.twcert.org.tw/tw/cp-132-8236-d4836-1.html

統睿科技DVC文件保險系統 - Arbitrary File Upload through Path Traversal	
TVN / CVE ID	TVN-202411018 / CVE-2024-11311
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	DVC 文件保險系統 6.0 至 6.3版本

問題描述	統睿科技DVC文件保險系統存在Path Traversal漏洞且未妥善驗證上傳檔案類型，未經身分鑑別之遠端攻擊者可上傳任意檔案至任意路徑，甚至可上傳網頁後門程式以執行任意程式碼。
解決方法	更新至6.4(含)以後版本
公開日期	2024-11-18
相關連結	https://www.twcert.org.tw/tw/cp-132-8246-d462a-1.html

統睿科技DVC文件保險系統 - Arbitrary File Upload through Path Traversal	
TVN / CVE ID	TVN-202411019 / CVE-2024-11312
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	DVC 文件保險系統 6.0 至 6.3版本
問題描述	統睿科技DVC文件保險系統存在Path Traversal漏洞且未妥善驗證上傳檔案任型，未經身分鑑別之遠端攻擊者可上傳任意檔案至任意路徑，甚至可上傳網頁後門程式以執行任意程式碼。
解決方法	更新至6.4(含)以後版本
公開日期	2024-11-18
相關連結	https://www.twcert.org.tw/tw/cp-132-8248-8dac9-1.html

統睿科技DVC文件保險系統 - Arbitrary File Upload through Path Traversal	
TVN / CVE ID	TVN-202411020 / CVE-2024-11313
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	DVC 文件保險系統 6.0 至 6.3版本
問題描述	統睿科技DVC文件保險系統存在Path Traversal漏洞且未妥善驗證上傳檔案任型，未經身分鑑別之遠端攻擊者可上傳任意檔案至任意路徑，甚至可上傳網頁後門程式以執行任意程式碼。
解決方法	更新至6.4(含)以後版本
公開日期	2024-11-18
相關連結	**https://www.twcert.org.tw/tw/cp-132-8250-1837b-1.html**

統睿科技DVC文件保險系統 - Arbitrary File Upload through Path Traversal	
TVN / CVE ID	TVN-202411021 / CVE-2024-11314
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	DVC 文件保險系統 6.0 至 6.3版本
問題描述	統睿科技DVC文件保險系統存在Path Traversal漏洞且未妥善驗證上傳檔案任型，未經身分鑑別之遠端攻擊者可上傳任意檔案至任意路徑，甚至可上傳網頁後門程式以執行任意程式碼。
解決方法	更新至6.4(含)以後版本
公開日期	2024-11-18
相關連結	**https://www.twcert.org.tw/tw/cp-132-8252-91d6a-1.html**

統睿科技DVC文件保險系統 - Arbitrary File Upload through Path Traversal	
TVN / CVE ID	TVN-202411022 / CVE-2024-202411022
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	DVC 文件保險系統 6.0 至 6.3版本
問題描述	統睿科技DVC文件保險系統存在Path Traversal漏洞且未妥善驗證上傳檔案任型，未經身分鑑別之遠端攻擊者可上傳任意檔案至任意路徑，甚至可上傳網頁後門程式以執行任意程式碼。
解決方法	更新至6.4(含)以後版本
公開日期	2024-11-18
相關連結	**https://www.twcert.org.tw/tw/cp-132-8254-8daa2-1.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：**2024年11月29 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/**