TWCERT/CC 資安情資電子報

2023 年 10 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 5 章節：

第 1 章、封面故事：上月 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。範疇包含資安趨勢、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、軟體系統資安議題、軟硬體漏洞資訊及新興應用資安。

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，此章說明上月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN)平台之漏洞嚴重程度前五的產品漏洞資訊。

第 5 章、資安情資分享概況：將上月份 TWCERT/CC 每日接收及分享之資安情資，針對對外資安情資分享地區及各項資安攻擊類型進行統計。

目錄

第 1 章、 封面故事

Chrome 擴充功能可用以竊取網站中的明文密碼

美國威斯康辛大學麥迪遜分校（University of Wisconsin–Madison）的資安研究人員團隊，近期發現一種攻擊方式，可以透過 Chrome 瀏覽器的擴充功能，竊取網站程式碼中儲存的使用者輸入密碼，且有不少擁有數百萬以上使用者的大型網站，將密碼以明文方式存在網頁 HTML 程式碼中。

該研究團隊已將其攻擊概念驗證程式編譯打包為 Google Chrome 擴充功能的格式，並上傳到 Chrome Web Store 中。

研究人員說，問題的根源在於開發人員在撰寫 Chrome 瀏覽器的擴充功能時，往往有個習慣性的做法，就是讓擴充功能能夠存取所有網頁會載入的 DOM 樹狀架構，而不會受到存取範圍的限制，因此導致擴充功能有機會存取到一些像是使用者輸入欄位之類的機敏資訊。

另外，擴充功能也可以濫用 DOM API 來跳過套用者網站上，用以保護機敏輸入資訊的各種資訊混淆機制，直接取得使用者輸入的值並加以竊取。

研究人員指出，雖然 Google 在 Manifest V3 協定已經針對 API 的取用加上限制，禁止擴充套件透過遠端取得程式碼的方式，來逃避資安偵測，並且避免以此方式遠端執行任意程式碼，但 Manifest V3 並未限制擴充套件

存取網頁內容的範圍，所以仍存有上述可竊得使用者輸入資訊的問題。

研究人員進一步指出，許多使用者眾多的大型網站，都會把使用者密碼以明文存在 HTML 源碼中，造成這類惡意擴充套件有可能竊得密碼；這些大型網站包括 gmail.com、cloudflare.com、facebook.com、citibank.com、irs.gov、capitalone.com、usenix.org、amazon.com 等。

建議網站開發人員應注意此問題，在撰寫程式碼時應嚴守資安最佳實務作法；使用者也應在各網站使用不同的強式密碼，並使用二階段登入驗證。

- 資料來源：
  1. Exposing and Addressing Security Vulnerabilities in Browser Text Input Fields
  2. Chrome extensions can steal plaintext passwords from websites

第 2 章、 國內外重要資安事件

2.1、資安趨勢

P2PInfect 僵屍網路透過各種隱形變種惡意軟體，活動量暴增 600 倍

資安廠商 Cado Security 近日發表研究報告指出，該公司旗下的資安研究人員調查發現，一個稱為 P2PInfect 的僵屍網路蠕蟲，自 8 月下旬起透過各種隱形變種惡意軟體，其駭侵攻擊活動量開始大量增加，9 月時增加到近 600 倍。

P2PInfect 的初次活動記錄是於 2023 年 7 月由資安廠商 Unit 42 所發現，該僵屍網路惡意軟體是一種對等網路 (Peer-to-peer，又稱 P2P) 架構，主要透過在直接連線網路的 Windows 或 Linux 主機上利用已知的遠端執行任意程式碼漏洞，植入 Redis 惡意軟體而進行擴散。

而在 2023 年 7 月底，Cado Security 的研究人員觀察到 P2PInfect 的全球活動量劇增；受到該惡意軟體駭侵的案例分布遍及全球；而受災最嚴重的國家則包括中國、美國、德國、新加坡、香港、英國、日本等國。

Cado Security 在報告中指出，由該公司設置的「蜜罐」(honeypot) 所截獲的惡意軟體活動，在今年 8 月到 9 月之間叫然上升達 600 之多；而 Cado Security 也發現多種不同的 P2PInfect 變種惡意軟體，顯示該惡意軟體的研發改版活動十分積極，能進行的駭侵攻擊活動類別也不斷增加，對資

安防護帶來更大的考驗。

有別於傳統主從式惡意軟體，需要設立少數控制伺服器來進行惡意軟體的酬載布署、資料收集等作業，P2PInfect 則利用對等式網路拓樸來分散作業，因此更加難以封鎖其攻擊網路。

Cado Security 指出，目前 P2PInfect 主要的攻擊酬載是安裝加密貨幣挖礦軟體，但目前並未觀察到實際的大規模挖礦運作，有可能只是駭侵者仍在進行實驗與測試，所以目前還不清楚 P2PInfect 布署的真正野心。

建議系統管理者與使用者必須隨時保持軟體安裝最新版本的資安修補程式，以免系統存有未修補的漏洞，遭此類惡意軟體入侵。

- 資料來源：
  1. Cado Security Labs Encounter Novel Malware, Redis P2Pinfect
  2. Cado Security Labs Researchers Witness a 600X Increase in P2Pinfect Traffic
  3. P2PInfect botnet activity surges 600x with stealthier malware variants

2.2、新興應用資安

2.2.1、CoinEx 加密貨幣交易所遭駭，損失達 5,300 萬美元

全球大型加密貨幣交易所 CoinEx 日前對外公開駭侵事件，該交易所的熱錢包遭駭侵攻擊，大量加密貨幣資金遭竊。

據 CoinEx 交易所在 X（原 Twitter）上發表的官方推文指出，該交易所的風險控制團隊在 2023 年 9 月 12 日發現數個該交易所擁有的熱錢包發生不正常提領狀況；該交易所目前正在調查事件發生原因與經過。

CoinEx 在推文中也指出，發生不正常提領的加密貨幣幣種，包括 Ethereum ($ETH)、Tron ($TRON) 和 Polygon ($MATIC)，但 CoinEx 也強調，所有客戶的數位資產都安全無虞且並未遭到攻擊；如有任何損失，都會得到 100% 的補償。

CoinEx 也表示，為加強安全防護並進行調查，暫時停止該所的加密貨幣入金與出金業務；待調查告一段落後就會儘快恢復服務。

雖然 CoinEx 並未在公開的訊息中提及此次駭侵事件造成的數位資產財務損失金額，但區塊鏈資安公司 PeckShield 指出，據該公司的監測資料，CoinEx 的損失包括 1,900 萬美元等值的 ETH、1,100 萬美元等值的 TRON（以 BSC 形式存於幣安的 Binance Smart Chain 上）、600 萬美元等值的 BTC、約 29.5 萬美元等值的 Polygon。

PeckShield 也表示，攻擊造成的數位資產損失約為 4,300 萬美元，而保

存在受攻擊錢包中的，另有 7,200 萬美元，已轉移到較為安全的冷錢包中；而另一家區塊鏈資安公司 CertiK Alert 估計的受害金額較高，達 5,300 萬美元。

建議加密貨幣相關業者與投資人，應對持有的數位資金安全性進行強化，資金勿長期存放於可連線存取的熱錢包中，以免因駭侵攻擊而造成鉅額損失。

- 資料來源：
  1. CoinEx Global @coinexcom
  2. PeckShieldAlert @PeckShieldAlert
  3. CertiK Alert @CertiKAlert
  4. Hackers steal $53 million worth of cryptocurrency from CoinEx

2.2.2、駭侵者假冒討債公司，攻擊 Celsius 加密貨幣借貸服務債權人

專業資安媒體 BleepingComupter 近日發表報導，指出近期有駭侵者以假冒不良債權追討業者 Stretto 的名目，接觸先前因加密貨幣貸款業者 Celsius 破產而導致權益受損的投資人，試圖竊取其加密貨幣錢包中的數位資產。

Celsius 是於 2022 年 7 月宣布破產倒閉的加密貨幣貸款業者，當時直接凍結使用者帳號的提款權限，造成許多人投入的資金無法領回，而 Stretto 是當時負責接受債權人處理 Celsius 破產後債權問題的業者。

據 BleepingComputer 的報導指出，近來許多債權人反應收到假冒 Stretto 發出的釣魚電子郵件，信中宣稱受害者只要填寫必須的資料欄位，將可在 7 日內收回被 Celsius 凍結的資金；而信中的連結會把使用者導向到疑似由駭侵者設立的釣魚網站，該釣魚網站的網域則註冊在塞席爾。

當債權人進入該釣魚網頁並輸入個人 email 地址後，會出現一個 WalletConnect 提示視窗，要求連結並存取債權人擁有的加密貨幣錢包；一旦同意，該釣魚網站即可取得加密貨幣錢包的各種資訊，包括錢包位址、餘額、資金進出記錄，並可建議進行交易。

BleepingComputer 進一步指出，一旦駭侵者用這種方法連線債權人的加密貨幣錢包，就可以偽造交易，假裝即將存入資金，事實上是將錢包中的加密貨幣與 NFT 提領一空。

BleepingComputer 的分析也指出，這波攻擊活動之所以能夠進行，是因為駭侵者找到方法，讓其發送的釣魚信件通過 Sender Policy Framework (SPF) 的郵件來源檢驗機制，因此不會被中間的郵件中繼伺服器阻擋下來。

建議加密貨幣投資人對於不明來源的錢包連線要求一定要特別提高警覺，勿輕易授權存取，以免資金遭到盜領。

- 資料來源：
  1. Pete No Stop @PeteNoStop
  2. Claimants in Celsius crypto bankruptcy targeted in phishing attack

2.2.3、Mixin Network 因遭駭 2 億美元而停止營運

開放源碼的點對點數位資產交易網路 Mixin Network 日前透過官方 Twitter 帳號宣布，因為一起近日發生的 2 億美元駭侵事件，該平台即日起暫停一切入金與出金相關交易。

該起駭侵事件發生於 2023 年 9 月 23 日香港時間清晨，Mixin Network 平台使用的的雲端服務廠商遭到駭侵者發動攻擊，導致主網上的部分數位資產遭到竊取。

Mixin 在事件發生後，已通報 Google 和區塊鏈資安廠商 SlowMist，共同調查整起事件；初步調查結果指出遭竊的資金約合 2 億美元。Mixin 也在推文中公告，在事件調查與漏洞修補完成前，暫停該網路的入金與出金業務，但轉帳業務不受影響。待調查與資安修補完成後，再行恢復正常運作。

而根據區塊鏈追蹤業者 PeckShield 與 Lookonchain 的監控報告指出，目前可確定的 1.41 億美元遭竊數位資產中，有 935 萬美元等值的以太幣、235 萬美元等值的 DAI、另外也有 233 萬美元等值的比特幣。

資安專家懷疑，Mixin Network 這次的竊案，可能又與專門攻擊區塊鏈與加密貨幣機構的 APT 駭侵團體 Lazarus 有關。光是在 2023 年度，Lazarus 針對加密貨幣已經高達 2.4 億美元，受害的加密貨幣相關服務包括 Atomic Wallet、Alphapo、Stake.com 和 CoinsPaid。

目前 Mixin Network 尚未提供具體的攻擊相關分析報告，整個駭侵事件的來龍去脈，目前仍不明朗。

建議加密貨幣投資人，務必將資金保管在離線的冷錢包中，並妥善保管存取短語，也應選擇具有資金保險的加密貨幣平台。

- 資料來源：
  1. Mixin Kernel @MixinKernel
  2. Mixin Network suspends operations following $200 million hack

2.3、國際政府組織資安資訊

2.3.1、奧克蘭大眾運輸系統管理中心疑因勒贖攻擊而癱瘓

紐西蘭第一大城奧克蘭 (Auckland) 大眾運輸系統 Auckland Transportation (AT) 的管理中心，日前因駭侵攻擊導致多數功能癱瘓，影響眾多服務無法正常運作。據了解，該駭侵攻擊可能屬於勒贖軟體的攻擊活動。

AT 是由紐西蘭奧克蘭市政府所控制的區域大眾運輸系統服務，主要服務範圍包括渡輪、碼頭、巴士、鐵路、公路與其他交通相關基礎設施。該公司在日前發表資安通報，指出由於不明原因，使其 HOP 服務 (即整合式的票券與運費系統) 發生運作障礙，具體發生的問題如下：

- HOP 交通卡的線上儲值與其他在 AT 網站上進行的 MyAT HOP 服務無法運作；
- 已發行的 HOP 交通卡可自動儲值，但付款流程發生延遲；
- 自動售票與儲值機僅能接受現金付款；
- 透過 Eftpos 和信用卡的交易發生障礙無法使用，部分機器也無法運作；
- AT 客服中心無法完全發揮功能，且只能收取現金付款；
- HOP 零售端點無法進行 HOP 卡片儲值或其他服務。

根據當地媒體 NZ Herald 報導指出，有一名 AT 官員表示有跡象指出，這次導致 AT HOP 系統異常的駭侵攻擊，係為勒贖攻擊；AT 則指

出，該單位正在逐一修復受影響的系統與服務，其官方網站與各項 HOP 服務系統，預計在數日後可以恢復運作。

不過 AT 並未透露具體的攻擊受損情形，以及攻擊者或攻擊手法等相關詳情；再者由於攻擊可能屬於勒贖攻擊，因此廣大乘客的個資是否會因而面臨資安風險，也成為外界關切的重點。目前並未有大型勒贖團體出面聲稱與該案件有關。

各公用事業由於手上擁有大量客戶資訊，且服務中斷恐造成嚴重衝擊與不便，建議應特別提高警戒，加強防範勒贖等各種形態駭侵攻擊。

- 資料來源：
  1. Public transport: Major cyber issue hits Auckland Transport's Hop card system, indications are it's a ransomware attack
  2. Auckland transport authority hit by suspected ransomware attack

2.3.2、百慕達政府遭駭侵攻擊

英國海外領土百慕達群島在日前遭到駭侵攻擊，導致其政府部門的所有 IT 系統、網路、email 與電話服務全面故障停用。

百慕達政府在與該攻擊相關的資安通報指出，該政府單位所有部門全面受到影響，無法正常提供服務；百慕達資訊與數位科技部目前正在努力進行修復，以求早日恢復政府單位正常機能。

百慕達總理 David Burt 在相關駭侵攻擊事件的記者會上指出，目前還沒有發現有任何百慕達政府相關資料遭竊的情報，且受這次駭侵事件影響波及的，除了百慕達以外，也包括加勒比海區域中的其他國家政府在內，且受影響的程度亦不在百慕達之下，不過 David Burt 並未表示是哪一個國家同樣遭到攻擊。

David Burt 表示，目前所得的初步分析結果指出攻擊源自百慕達境外。該地政府目前正與相關資安單位合作，以確認攻擊造成的影響與其範圍，並且盡早恢復政府單位正常運作。

百慕達政府在稍後補充說明指出，該地政府僱員的薪資與包商費用的結算撥款，可能因此攻擊事件而有所延誤，目前百慕達政府的財會單位僅能處理現金與支票，無法使用電腦系統。

除了政府行政單位之外，百慕達群島的下議院（House of Assembly）也因此次攻擊活動而無法按既定計畫，在休會結束後開議。

目前百慕達警察單位未受影響，仍可照常執行各項治安維持工作；百慕達政府也要求所有公務人員正常上班，以確保政府服務仍可盡力維持。

建議各政府單位須加強資安防護作業，避免各種境外勢力發動攻擊，導致政府失能。

- 資料來源：
  1. Bermuda Government @BdaGovernment
  2. Russia linked to cyberattack on government services
  3. Government of Bermuda links cyberattack to Russian hackers

2.4、社群媒體資安近況

2.4.1、勒贖攻擊團體 Key Group 透過 Telegram 散布惡意軟體

資安廠商 EclecticIQ 日前發表研究報告，指出該公司旗下的資安人員，發現的新勒贖攻擊團體 Key Group 透過 Telegram 頻道散播惡意軟體，不但會對受害者設備中的資料進行加密，且還會竊取受害者的個人機敏資訊。

報告指出，Key Group 的主要目的應為藉勒贖攻擊斂財。主要的攻擊對象為俄羅斯境內的受害者。該團體除了要求受害者償付贖金外，也會在一個名為 Dark Store 的俄羅斯暗網中販賣用戶個資與其社群帳號、VPN 帳密和 email 地址。

EclecticIQ 是在 2023 年 1 月 6 日起觀測到 Key Group 的相關攻擊活動，並持續活動至今。資安研究人員發現 Key Group 的成員利用 Telegram 中的頻道 keygroup777Tg 來進行攻擊活動與贖金要求。另外該團體還有一個私密 Telegram 頻道，用以協調成員間的攻擊行動，並共享各種工具的資訊。

EclecticIQ 指出，該團體有可能自 6 月底開始利用一種稱為 NjRAT 的遠端遙控工具，來控制受害者的裝置。

報告也指出，Key Group 使用一種 CBC-mode 進階加密標準 (AES) 來加密受害者的資料，並將用戶的檔案名稱加上 keygroup777tg 的副檔名。由

於這種加密方式並不太複雜，加上該團體的駭侵技術並不強，在進行加密時犯了一些技術上的錯誤，因此 EclecticIQ 已經利用這些錯誤，開發出針對其 8 月 3 日版本勒贖軟體的解密工具。

為避免遭到勒贖攻擊，建議使用者避免點按不明來源如釣魚郵件、社群頻道或聊天軟體中傳送的連結。

- 資料來源：
  1. Decrypting Key Group Ransomware: Emerging Financially Motivated Cyber Crime Gang
  2. Free Decryptor Available for ‘Key Group’ Ransomware

2.4.2、TikTok 上充斥假冒 Elon Musk 的加密貨幣發放詐騙攻擊

資安專業媒體 BleepingCompter 日前發表一篇專題報導，指出短影音社群媒體平台 TikTok 上，目前大量出現假冒 Elon Musk 旗下知名企業如 Tesla、Space X 等的加密貨幣發放詐騙攻擊，使用者應特別提高警覺。

報導指出，這類假冒名人在社群平台上，以發放加密貨幣為詐騙誘餌的案例，近年來層出不窮，並不是新穎的詐騙手法；這類詐騙總是假冒科技界或幣圈知名人士的身分，在社群媒體上張貼詐騙貼文，宣稱只要使用者以加密貨幣進行匯款，就可以得到倍數的加密貨幣回饋，以此吸引不察的使用者上當受騙。

詐騙者通常會設立數百個網站，假冒為加密貨幣發送活動網站或加密貨幣交易所，要求受害者註冊帳號，並進行匯款以收取免費發放的加密貨幣；但所有這類案例的結果都完全相同，就是受害者的匯款遭到騙取，完全無法領到「發放」的加密貨幣獎金。

BleepingComupter 專文指出，過去這類詐騙案多半出現在 Facebook、Instagram、Twitter 和 YouTube 上，而由於 TikTok 的快速崛起，也成為詐騙者愛用的社群平台。近來的案例多半是以 Elon Musk 過去接受電視新聞專訪的影片為素材，利用深偽技術，將 Musk 受訪的談話內容，偷換成加密貨幣詐騙的宣傳，用以誘騙受害者上當。

也有一些詐騙活動的影片製作技術較為粗糙，內容是如何在詐騙網站上註冊的流程，以獲得免費的加密貨幣。

建議加密貨幣投資者對這類明顯過度好康的活動，均應提高警覺，不要任意點按連結或參與活動。

- 資料來源：
  1. Verified Twitter accounts hacked in $580k ‘Elon Musk’ crypto scam
  2. TikTok flooded by 'Elon Musk' cryptocurrency giveaway scams

2.4.3、通訊軟體 Signal 推出可對抗量子電腦運算的端對端加密演算法

全球大型即時通訊服務平台 Signal 日前宣布推出全新的端對端加密 (End-to-end encryption, E2EE) 通訊協定，使用一種全新加訊息加密演算法，據稱能夠對抗量子電腦極為高速度的破解運算。

量子電腦是一種利用量子效應與量子位元進行運算的全新電腦架構，能夠在極短時間內，以平行處理方式進行極高速的運算，效能可達傳統高速電腦的一億倍以上；傳統加密演算法以傳統電腦進行破解運算，如需數十年到數百年時間破解，量子電腦可能僅需數秒即可運算完成，因此對傳統加密演算法構成極為嚴重的考驗。

目前雖然量子電腦仍處於實驗階段，僅有大型研究機構與電腦公司有能力進行研發製造，但資安界已預見其威脅；一旦駭侵者掌握量子電腦的超級算力，各種現行資安保護機制勢將瓦解。

Signal 指出，其原本使用的「X3DH」(Extended Triple Diffie-Hellman) 金鑰聚合通訊協定，在今後將升級為「PQXDH」(Post-Quantum Extended Diffie-Hellman) 演算法，該演算法同時採用 X3DH 的橢圓曲線金鑰同意協定，以及稱為 CRYSTALS-Kyber 的抗量子運算金鑰包裝機制。CRYSTALS-Kyber 是一種已獲美國 NIST 認證的加密演算法，適用於一般性與需要快速交換小型加密金鑰的加密解密運算需求。

SIgnal 指出，該公司並未計畫直接以新的 PQXDH 抗量子運算加密協定取代現有的 X3DH 加密協定，而是逐步過渡到各種抗量子運算的新加密

演算法；未來將會推出更多的升級與調整，以對應日益嚴重的資安挑戰。

為因應量子電腦強大算力可能落入駭侵者控制的危機，建議各公私單位應思考對抗量子運算的方法與新技術，並擬定導入計畫，強化資安防護能力。

- 資料來源：
  1. Quantum Resistance and the Signal Protocol
  2. The PQXDH Key Agreement Protocol
  3. Signal adds quantum-resistant encryption to its E2EE messaging protocol

2.5、行動裝置資安訊息

2.5.1、Apple 緊急修復 2 個已遭用於攻擊的 iMessage 0-day 漏洞

Apple 於近日為旗下的 iPhone 與 Mac 產品推出緊急更新，修復兩個已遭駭侵者用於攻擊的 iMessage 0-day 漏洞 CVE-2023-41064 與 CVE-2023-41061。

這兩個 0-day 漏洞都存於 iOS 與 macOS 的 Image I/O 與 Wallet Framework 之中，其中 CVE-2023-41064 屬於緩衝區溢位錯誤，駭侵者可利用特製的圖片檔案來誘發此漏洞發生錯誤，藉以執行任意程式碼。

而 CVE-2023-41061 的 0-day 漏洞則屬於驗證錯誤，駭侵者可使用特製的夾檔來誘發此錯誤，同樣可在受攻擊裝置上執行任意程式碼。

發現 CVE-2023-41064 漏洞的資安廠商 Citizen Labs 指出，該公司的資安人員已發現這兩個 0-day 漏洞遭一個名為「BLASTPASS」的駭侵攻擊行動加以濫用，可在無需使用者互動的情形下，於受攻擊的裝置上布署 NSO Group 的 Pegasus 間諜軟體。

Apple 在針對這兩個 0-day 漏洞發表的資安通報上也指出，該公司已獲悉這兩個漏洞已遭駭侵者積極運用於攻擊活動的情報。

Apple 已推出修復此兩個 0-day 漏洞 CVE-2023-41064 與 CVE-2023-41061 的更新版作業系統，包括 macOS Ventura 13.5.2、iOS 16.6.1、iPadOS 16.6.1、WatchOS 9.6.2；受影響的硬體裝置則包括 iPhone 8 與後續機型、

iPad Pro（所有機型）、iPad Air 第 3 代與後續機型、iPad 第 5 代與後續機型、iPad mini 與後續機型，以及所有執行 macOS Ventura 的 Mac 電腦、Apple Watch Series 4 與後續機型。

建議相關產品用戶立即更新至最新版本作業系統，以免遭到駭侵者利用未修補漏洞攻擊而造成損失。

- 資料來源：
  1. Bill Marczak @billmarczak
  2. About the security content of iOS 16.6.1 and iPadOS 16.6.1
  3. Apple discloses 2 new zero-days exploited to attack iPhones, Macs

2.5.2、APT36 駭侵團體以假冒 YouTube App 感染 Android 行動裝置

資安廠商 SentinelLabs 日前發表研究報告，指出該公司旗下的資安專家，近期發現 APT 駭侵團體 APT36，利用至少 3 個冒充為 YouTube 的 Android App 來散布遠端遙控木馬惡意軟體 CapraRAT。

據 SentinelLabs 的報告指出，APT36 又名「Transparant Tribe」（透明部落），慣用手法為透過特製的 Android App 上架到第三方 Andoird App Store 中，針對印度的國防軍事與政府單位進行攻擊。

SentinelLabs 指出，這次觀測到的攻擊行動，主要的攻擊目標是印度與軍事外交事務相關的單位或個人，攻擊手法是利用社交工程方式，針對攻擊目標散布至少三種假冒為 YouTube App 的惡意 APK 軟體。三個惡意軟體中有兩個就名為「YouTube」，另一個則稱為「Piya Sharma」，利用這個和愛情故事相關的名字來發動「羅曼史攻擊」。

這些惡意軟體的介面都模仿真正的 YouTube App，但卻是使用 WebView 而非原生軟體介面，另外也缺少真實 App 擁有的部分功能。

一旦使用者誤裝了這三種惡意軟體，CapraRAT 就會背景執行各種攻擊，包括竊取前後相機與麥克風接收到的影像與聲音、竊取簡訊內容與通話記錄、擅自發送簡訊並阻擋來訊、擅自撥號通話、竊取螢幕截圖、擅自覆蓋系統設定值、竄改手機中的檔案等等。

SentinelLabs 也指出，Transparant Tribe 經常進行惡意軟體改版，以持

續監控並攻擊印度與巴基斯坦境內的目標。

建議 Android 使用者避免自不明來源如第三方應用程式商店、email 或社群媒體點按連結並安裝 APK 檔案，以免安裝到內含惡意軟體的假 App。

- 資料來源：
  1. CapraTube | Transparent Tribe's CapraRAT Mimics YouTube to Hijack Android Phones
  2. APT36 state hackers infect Android devices using YouTube app clones

2.5.3、來電辨識軟體遭駭侵團體變造植入惡意軟體

資安廠商 Volexity 日前發表研究報告，指出該公司旗下的研究人員，近日發現一個名為 EvilBamboo 的駭侵團體，利用在多種 Android App 中植入惡意軟體 Badsignal、BadBazaar、BadSolar 等家族的手法，針對 Android 使用者與組織發動攻擊。

Volexity 在報告中指出，該公司追蹤 EvilBamboo 的駭侵攻擊行動，期間長達 5 年以上；該駭侵團體長期針對 Android 平台開發出多種惡意軟體，包括 BadBazaar、BadSignal、BadSolar 等。

在攻擊台灣的部分，Volexity 在報告中指出，EvilBamboo 將其研發的 BadBazaar 惡意軟體植入到來電辨識阻擋軟體 Android 版，並以可免費使用完整功能的破解版 Whoscall 為號召，將惡意竄改過的 Whoscall APK 檔透過如 apk.tw 等 Android 軟體相關論壇來散布。

在 apk.tw 上該篇貼文內容雖然已遭刪除，貼文者亦被停權，但該篇文章的點閱次數超過 10 萬次以上；而據 Veloxity 的報告指出，BadBazaar 惡意軟體具有竊取使用者簡訊內容、電信業者服務資訊與入侵裝置詳細資訊，甚至也能自動進行更新。

而在針對其他攻擊對象方面，EvilBamboo 也會利用如 Telegram、假冒網站等各種方式來散播惡意軟體，吸引被害者下載安裝到手機上，以進行進一步的攻擊活動。

建議行動裝置使用者不要自官方 App Store 之外的不明來源管道自行安裝軟體，避免成為惡意軟體的散播傳染對象。

- 資料來源：
  1. EvilBamboo Targets Mobile Devices in Multi-year Campaign
  2. 來電辨識 v7.45 付費破解版+版本自動更新

2.5.4、Apple 緊急修復 3 個已用於攻擊的 macOS/iOS 0-day 漏洞

Apple 日前緊急推出 iOS/macOS/iPadOS 和 watchOS 更新，解決 3 個已遭用於駭侵攻擊的 0-day 漏洞，用戶應立即更新相關裝置內的舊版作業系統，以免遭到駭侵者利用已知漏洞發動攻擊得逞。

在這次發現的 3 個 0-day 漏洞中，第一個 CVE-2023-41993 係存於 WebKit 瀏覽器引擎內，第二個 CVE-2023-41991 則存於資安框架 (Security framework) 中；駭侵者可利用特製的網頁來誘發這兩個漏洞發生錯誤，藉以跳過數位簽署驗證機制以執行惡意 App，或是用以執行任意程式碼。

第三個漏洞 CVE-2023-41992 存於核心框架（Kernel Framework）中；核心框架提供 API 與支援，以供核心擴充套件與存於核心的裝置驅動程式使用。本地駭侵者可利用此漏洞來提升執行權限。

Apple 在發布的資安通報中指出，該公司已接獲這三個漏洞已遭駭侵者攻擊 iOS 16.7 之前版本作業系統的情資。

受到影響的裝置如下：

- iPhone 8 與後續機型；
- iPad mini (第 5 代) 與後續機型；
- 執行 macOS Montery 與後續版本的 Mac 電腦；
- Apple Watch Series 4 與後續機型。

Apple 緊急推出的作業系統新版本為 macOS 12.7/13.6、iOS 16.7/17.0.1、iPadOS 16.7/17.0.1、watchOS 9.6.3/10.0.1；上述機型的使用者應立即更新系統，以避免遭到駭侵者利用已知漏洞發動攻擊。

- 資料來源：
  1. About the security content of macOS Ventura 13.6
  2. Apple emergency updates fix 3 new zero-days exploited in attacks

2.6、軟體系統資安議題

2.6.1、12,000 台 Juniper 網通產品內含嚴重 RCE 漏洞

資安專家估計，市面上約有 12,000 Juniper SRX 防火牆裝置與 EX 系列交換器，內含一個嚴重的資安漏洞，駭侵者可透過該漏洞，無需檔案和登入驗證，即可遠端執行任意程式碼。

在 2023 年 8 月時，Juniper 自行在資安通報中公開了數個 PHP 環境變數操弄的漏洞，包括 CVE-2023-36844、CVE-2023-36845，以及數個關鍵功能無需登入驗證的漏洞，包括 CVE-2023-36846、CVE-2023-36847。當時這些漏洞的 CVSS 危險程度評分較低，僅有 5.3 分（滿分為 10 分），危險程度評級為「中等」（medium）。

然而資安專家發現，可以把這些漏洞組合成一個更危險的資安漏洞，用以遠端執行任意程式碼；這使得合成漏洞的危險程度評分立即上升到 9.8 分；甚至可以在無需上傳任何檔案的情況下，僅僅利用 CVE-2023-36845 這個單一漏洞，就能在受攻擊裝置上遠端執行任意程式碼。

資安廠商 VulnCheck 在近期發表的研究報告中，公開了該公司旗下資安專家發展出的概念攻擊證明（PoC）流程；該流程可利用 GitHub 上可免費取得使用的掃瞄工具，在開放網路上找到 12,000 台以上含有此漏洞的 Juniper 網路裝置加以攻擊。

受 CVE-2023-36845 漏洞影響的 Juniper 網通產品，包括執行下列版本 Junos OS 的 EX 與 SRX 系列機型：

- 20.4R3-S8 先前所有版本
- 21.1 版本 21.1R1 與後續版本
- 21.2R3-S6 先前的 21.2 版本
- 21.3R3-S5 先前的 21.3 版本
- 21.4R3-S5 先前的 21.4 版本
- 22.1R3-S3 先前的 22.1 版本
- 22.2R3-S2 先前的 22.2 版本
- 22.3R2-S2、22.3R3 先前的 22.3 版本
- 22.4R2-S1、22.4R3 先前的 22.4 版本

Juniper 已在日前釋出更新版本，但網路上仍有眾多受影響設備仍未及更新。

建議系統管理員應時時注意各軟硬體設備的漏洞與更新消息，並於第一時間套用更新，以免遭駭侵者透過已知但未修補的漏洞發動攻擊。

- 資料來源：
  1. Fileless Remote Code Execution on Juniper Firewalls
  2. 2023-08 Out-of-Cycle-Security-Bulletin：Junos-OS-SRX-Series-and-EX-Series：Multiple-vulnerabilities-in-J-Web
  3. Thousands of Juniper devices vulnerable to unauthenticated RCE flaw

2.6.2、Xenomorph Android 惡意軟體針對多國銀行與加密貨幣錢包發動攻擊

資安廠商 ThreatFabric 旗下的資安研究人員，近期發現一個稱為 Xenomorph 的 Android 惡意軟體，近來再次大舉針對世界各國多家銀行與加密貨幣錢包發動攻擊。

ThreatFabric 的研究人員，自 2022 年 2 月開始追蹤 Xenomorph 的駭侵活動，當時發現該惡意軟體透過 Google Play Store 中上架的 App 進行散布，下載次數多達 50 萬次以上，攻擊對象則為歐洲各國的 56 家銀行。

該惡意軟體的始作俑者 Hodoken Security 持續不斷進行 Xenomorph 的改版，自 2022 年 6 月後 Xenomorph 進行重構，讓 Xenomorph 具備模組化功能，變得更具有彈性；而在 2023 年 3 月，Hadoken 再次對 Xenomorph 進行改版，在該惡意軟體中加入自動轉帳系統、跳過多階段登入驗證、cookie 竊取等功能，且有能力攻擊超過 400 家銀行。

ThreatFabric 指出，在最新一波的攻擊行動中， Xenomorph 利用假冒的 Android 內建瀏覽器 Chrome 的升級通知，誘騙使用者下載安裝植入了 Xenomorph 的 APK 檔案，接著 Xenomorph 便可在使用者瀏覽金融機構或加密貨幣錢包頁面時，使用畫面覆疊來竊取使用者輸入的登入資訊。

ThreatFabric 也指出，過去 Xenomorph 以攻擊歐洲的金融機構為主，而在這波攻擊中，美國的金融機構也納入其攻擊範圍內，成為該惡意軟體最主要的受害地區。其他受害地區還包括西班牙、加拿大、義大利、葡萄牙、比利時等。

建議 Android 使用者避免在官方 App Store 之外場合安裝來路不明的 APK 檔案，也應對要求過多使用權限的 App 提高警覺。

- 資料來源：
  1. Xenomorph Malware Strikes Again: Over 30+ US Banks Now Targeted
  2. Android malware Xenomorph runs new campaign targeting the U.S.

2.6.3、駭侵者利用近期已更新的 Apple、Google Chrome 0-day 漏洞攻擊埃及總統候選人

資安廠商 Citizen Lab 與 Google 旗下的資安研究機構 Threat Analysis Group (TAG)，近日發現 Apple 與 Google Chrome 日前修復的數個 0-day 漏洞，已遭駭侵者用於各種攻擊活動之上；使用者應立即更新系統。

Apple 日前緊急推出 iOS/iPadOS/macOS/watchOS 的更新版本，修復 3 個 0-day 漏洞，分別是 CVE-2023-41991、CVE-2023-41992、CVE-2023-41993；但根據資安廠商 Citizen Lab 的觀測報告指出，在 2023 年 5 月到 9 月之間，有駭侵者利用這三個漏洞，使用特製的惡意簡訊與 WhatsApp 訊息，在埃及前任國會議員 Ahmed Eltantawy 宣布參與 2024 年埃及總統選舉後，針對該政治人物發動資安攻擊。

Citizen Lab 在報告中指出，攻擊者事先入侵 Eltantawy 使用的埃及電信業者 Vodafone，然後在 Eltantawy 瀏覽非 https 加密的網站時，利用已駭入的電信業者設備，將其導向到一個惡意網站，並在其 iPhone 手機中安裝 Cytrox 製作的惡意間諜軟體 Predator。

此外，Google 旗下的 TAG 也發現有攻擊者利用近期已獲更新的 Chrome 漏洞 CVE-2023-4762，在埃及境內的 Android 裝置中植入 Predator 間諜軟體。該漏洞可讓駭侵者遠端執行任意程式碼。

Apple 呼籲所有使用者盡快更新到最新版本作業系統，對於可能成為攻擊對象的高度敏感人士，應在有必要時啟用手機內建的「封閉模式」；這個模式會嚴格限制各種網路資源的使用，可大幅提高裝置使用的安全

性。

針對高度可能遭到攻擊的對象，其資訊裝置除應時時更新到最新版本作業系統外，且在必要時應使用封閉模式，以達最高等級的安全性。

- 資料來源：
  1. Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions
  2. John Scott-Railton @jsrailton
  3. Recently patched Apple, Chrome zero-days exploited in spyware attacks

2.7、軟硬體漏洞資訊

2.7.1、Microsoft 推出 2023 年 9 月 Patch Tuesday 每月例行更新修補包，共修復 59 個資安漏洞，內含 2 個 0-day 漏洞

Microsoft 日前推出 2023 年 9 月例行資安更新修補包「Patch Tuesday」，共修復 59 個資安漏洞；其中含有 2 個是屬於已遭駭侵者用於攻擊的 0-day 漏洞。

本月 Patch Tuesday 修復的漏洞數量有 59 個，較上個月（2023 年 8 月）的 87 個資安漏洞略為減少；而在這 59 個漏洞中，僅有 5 個屬於「嚴重」等級，另有 2 個是屬於已知遭到駭侵者用於攻擊的 0-day 漏洞，另外還有 24 個遠端執行任意程式碼 (RCE) 漏洞。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 資安防護功能略過漏洞：3 個；
- 遠端執行任意程式碼漏洞：24 個；
- 資訊洩露漏洞：9 個；
- 服務阻斷（Denial of Service）漏洞：3 個；
- 假冒詐騙漏洞：5 個；
- Edge -Chromium 漏洞：5 個。

本月的 Patch Tuesday 有 2 個已遭大規模濫用的 0-day 漏洞：

第一個 0-day 漏洞是 CVE 編號為 CVE-2023-36802，存於 Microsoft Streaming Service Proxy 中，屬於執行權限提升漏洞；駭侵者可透過此漏洞，將自身的執行權限提高的系統（system）等級。

第二個值得注意的 0-day 漏洞是 CVE-2023-36761，是存於 Microsoft Word 中的資訊洩露漏洞，駭侵者可利用此漏洞，在開啟檔案或預覽檔案內容時，竊取 NTLM 雜湊資訊，進一步用於透過 NTLM 中繼攻擊，最後可以取得帳號的控制權。

- CVE 編號：CVE-2023-36802、CVE-2023-36761
- 影響產品(版本)：Microsoft 旗下多種軟體，包括 Windows、Office、Exchange 等。
- 解決方案：建議系統管理者與 Microsoft 用戶依照指示，套用 Patch Tuesday 與不定期發表的資安更新，以避免駭侵者利用未更新的漏洞發動攻擊。

- 資料來源：
  1. Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
  2. Microsoft Word Information Discolsure Vulnerability
  3. Microsoft September 2023 Patch Tuesday fixes 2 zero-days, 59 flaws

2.7.2、趨勢科技修復 Apex One 端點保護解決方案的 0-day 漏洞

資安大廠趨勢科技 (Trend Micro) 近期修復一個存於其 Trend Micro Apex One 端點保護解決方案的 0-day 漏洞 CVE-2023-41179；該漏洞證實已遭積極用於駭侵攻擊活動。

Trend Micro Apex One 端點保護解決方案是針對各種大中小型企業資安需求設計的資安防護系統，而該 0-day 漏洞 CVE-2023-41179 存於 Apex One 來自第三方的反安裝 (uninstall) 模組內，駭侵者可利用該漏洞來執行任意程式碼。

受此漏洞影響的 Trend Micro 產品如下：

- Trend Micro Apex One 2019
- Trend Micro Apex One SaaS 2019
- Worry-Free Business Security (WFBS) 10.0 SP1 (在日本以 Virus Buster Business Security (Biz) 之名發行)
- Worry-Free Business Security Services (WFBSS) 10.0 SP1 （在日本以 Virus Buster Business Security Services (VBBSS) 之名發行）

該漏洞的 CVSS 危險程度評分高達 9.1 分（滿分為 10 分），危險程度評級亦為最高等級的「嚴重」（Critical）。日本電腦網路危機處理暨協調中心（JPCERT/CC）也對此漏洞發布資安通告，敦促所有使用受影響版本的用戶，應立即更新到最新版本。

Trend Micro 在下列最新版本中，已修復此漏洞：

- Apex One 2019 Service Pack 1 – Patch 1 (Build 12380)
- Apex One SaaS 14.0.12637
- WFBS Patch 2495
- WFBSS July 31 update

- CVE 編號：CVE-2023-41779
- 影響產品(版本)：Trend Micro Apex One 2019、 Trend Micro Apex One SaaS 2019、 Worry-Free Business Security (WFBS) 10.0 SP1 (在日本以 Virus Buster Business Security (Biz) 之名發行)、 Worry-Free Business Security Services (WFBSS) 10.0 SP1 （在日本以 Virus Buster Business Security Services (VBBSS) 之名發行）。
- 解決方案：建議使用上述版本的用戶，應立即更新到新版本。

- 資料來源：
  1. CRITICAL SECURITY BULLETIN: 3rd Party AV Uninstaller Module for Trend Micro Apex One and Worry-Free Business Security Arbitrary Code Execution Vulnerability
  2. Alert Regarding Vulnerability in Trend Micro Multiple Endpoint Security Products for Enterprises
  3. Trend Micro fixes endpoint protection zero-day used in attacks

2.7.3、Mozilla 緊急修補 Firefox、Thunderbird 已遭用於駭侵攻擊的 0-day 漏洞

Mozilla 日前針對一個證實已遭用於駭侵攻擊的 Firefox、Thunderbird 0-day 嚴重漏洞推出緊急修補更新，使用者應立即套用。

該 0-day 漏洞的 CVE 編號為 CVE-2023-4863，是存於 WebP 程式碼儲存庫 (libwebp) 中的一個 heap 緩衝區在處理內容時發生的溢位錯誤；駭侵者可誘使受害者開啟特製的 WebP 影像檔案，藉以觸發該漏洞，造成系統崩潰，即可執行任意程式碼。

CVE-2023-4863 漏洞的 CVSS 漏洞危險程度評分達 8.8 分（滿分為 10 分），危險程度評級為「高」。Mozilla 也在對外發表的資安通報中指出，該公司已獲悉此漏洞已遭駭侵者用於攻擊活動的情資。

針對此一高風險 0-day 漏洞，Mozilla 推出 Firefox 117.0.1、Firefox ESR 115.2.1、Firefox ESR 102.15.1、Thunderbird 102.15.1 與 Thunderbird 115.2.2 新版。

此外，雖然 CVE-2023-4863 主要是發生在 Mozilla 推出的瀏覽器相關產品，但受此漏洞影響的軟體並不限於 Firefox 與 Thunderbird 等 Mozilla 產品；只要使用了 WebP 程式庫程式碼的應用程式，都含有此漏洞，包括 Google Chrome 瀏覽器在內。

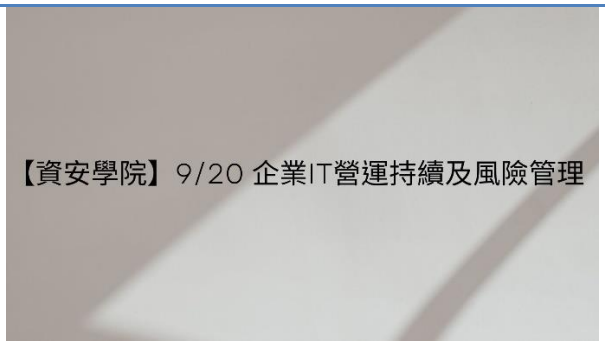
Google Chrome 也已在近日針對 CVE-2023-4863 推出更新修補，但目

前僅限於 beta 測試版；要再過數日到數星期，這個更新才會推送到一般使用者使用的 Stable 版本和 Extended Stable 版本。

- CVE 編號：CVE-2023-4863
- 影響產品(版本)：
- 解決方案：建議上述 Mozilla 軟體的使用者應立即透過系統更新程序，更新到最新版本，以免遭到駭侵者透過未修補的已知漏洞發動攻擊得逞。

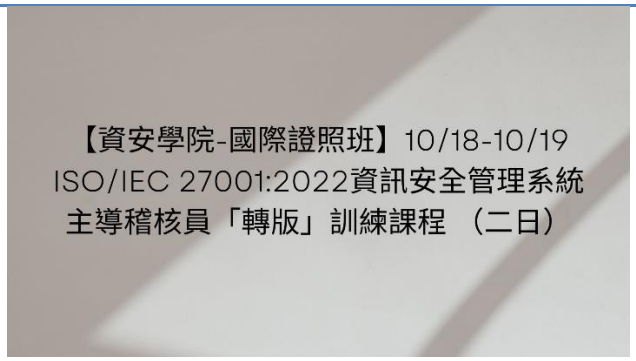
- 資料來源：
  1. Mozilla Foundation Security Advisory 2023-40
  2. CVE-2023-4863

第 3 章、 資安研討會及活動

【資安學院】10/16 企業 IT 營運持續及風險管理	
活動時間	**2023-10-06(一) 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/3962**
活動概要	 **主辦單位：中華民國資訊軟體協會** 費用： -原價 6,900/人 -早鳥價 6,200/人 -軟協會員 5,600/人 -費用含稅、教材及完課證明 活動內容 / Event Details： 身處資訊發展迅速的年代，企業運用科技生產先進的產品、提供客戶即時便利的服務、追求更高利潤的同時，風險的發生已經超越了以往，如資訊系統大當機、駭客入侵、勒索病毒等層出不窮，這些災害可能使得人員作業或資訊設備中斷，造成企業的重大危機。 營運持續策略是目前業界應對的有效管理機制，鑑別出威脅組織的潛在衝擊，提供具有彈性的應對計畫，以維持組織 IT 的持續運作。本課程採用互動式教學，引用目前業界之實務作法，提升學員分析及規

	劃能力。 聯絡窗口： 02-2553-3988 分機 388　廖資深專員 security@cisanet.org.tw <mailto:security@cisanet.org.tw> 報名截止： 2023-10-10

【資安學院】10/17 洞察 web3.0 的數位商機：踏上區塊鏈實用技術與應用之路	
活動時間	**2023-10-17 13:30 ~ 2023-10-17 16:30**
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/5120**
活動概要	 **主辦單位：中華民國資訊軟體協會** web3.0 是軟體開發者的天堂，但新技術演進飛快，市場變動眼花撩亂，在此紛亂的資訊中，如何發掘機會，實踐驗證，並且得到立足成功，是建造者所追求的成功經驗，也是創業者最感興趣的部分！ 講者分享自身在 web2.0 到 web3.0 軟體世界的歷程，以及在 web3.0 資本市場裡面的親身經歷，希望給聽眾有一個可複製的途徑，在短期之內就可以取得 web3.0 立足機會！ 聯絡窗口： 02-2553-3988 分機 388、816　廖資深專員、林專員 security@cisanet.org.tw 報名截止： 2023-10-12

【資安學院-國際證照班】10/18-10/19 ISO/IEC 27001:2022 資訊安全管理系統 主導稽核員「轉版」訓練課程（二日）	
活動時間	2023-10-18 09:00 ~ 2023-10-19 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/4031**
活動概要	 **主辦單位：中華民國資訊軟體協會** ISO 27001 隨著數位化改變全球數位格局，如遠端工作、自攜電子設備以及工業 5.0 等商業實務，變得更佳依賴雲端和數位。ISO/IEC 27001 於 2022 年 10 月 25 日正式頒佈新版標準（2022 年版），其中有些更動如編輯小幅更動、為符合新的 ISO 調和結構的更動，以及在安全控制面的要求進行了許多新增及調整。 此課程主要是針對已上過 ISO/IEC 27001:2013 年版的學員，提供新舊版本標準的差異介紹，以協助學員能有效的提升對新版標準的瞭解。通過考試者，將由 BSI 英國標準協會台灣分公司授予轉版證書。 費用： 原價：NT 24,000 元/人 軟協會員：NT 22,000 元/人 早鳥價：NT 23,500 元/人(8/18 前需完成報名及繳費) 四人團報價：NT23,000 元/人 費用含稅、教材、餐點及證書

	聯絡窗口： 02-2553-3988 分機 388　廖資深專員 security@cisanet.org.tw 報名截止： 2023-10-13

探索未來世代的網路隱私治理框架	
活動時間	**2023 年 10 月 18 日(三) , 14:00-16:00**
活動地點	**IEAT 國際會議中心 11 樓第一會議室/Webex 會議室** ******本活動採實體與線上同步進行******
活動網站	**https://www.twsig.tw/20231018/**
活動概要	 **主辦單位：TWNIC、NII、TWIGF** 許多孩子在出生前就早開始在數位世界中曝光，從超音波照片、牙牙學語短影音、幼兒園生活照、出國旅行機票、國小班級部落格圖文、國中畢業旅行大合照，到高中社團表演精彩片段影片，隨著孩子成長，這些文字、圖像、影片，連同孩子的名字、學校制服、生活經驗一起被記錄及上傳至各式的社群網站或影音平台。求學過程中，孩子們在校園中註冊使用的是商業公司提供的教育版電子郵件與免費線上教學服務；青少年階段，為了與同儕討論時下流行趨勢，他們提供個人資料註冊了各種短暫出現的線上服務，眼球停留在大量短影音上。 大量屬於兒童與青少年的個人資料在數位世界中不斷被蒐集，不只是由家長自作主張地釋出，還包括他們自己主動提供的個資，以及瀏覽這些線上服務時留下的各種數位足跡。與一般成人的網路資料保護最大的區別是，他們通常對於個人資料送出後可能的風險、後果或保護措施不夠理解，也因為其年齡或其他限制，而無機會或管道表達出自己的想法與主張。 本座談會將探討兒少使用各式線上服務時，資料蒐集端與兒少之間的權力不平衡課題，以及如何藉由如透明度等機制來處理兒少的個人隱私資料，檢視當前網路服務提供商對於兒少個資的政策內涵，衍生的問題與案例，並試著就如何優先考量兒少利益來建立一個以兒少為中心的資料治理或隱私框架建議。

【資安學院】10/25 程式碼掃描修補安全	
活動時間	**2023-10-25 14:00~17:00**
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/4007**
活動概要	 **主辦單位：** 系統上線前執行源碼掃描安全檢測已是常見檢測作業，檢測工具所顯示之弱點與實際程式的架構不同，真的代表有這個漏洞存在嗎？ 本課程透過實務案例分析常見漏洞教學，原始碼掃描修補邏輯判斷的原則，並透過實務教學 OWASP TOP 10 掃描風險修補技巧。 聯絡窗口： 02-2553-3988 分機 388、816　廖資深專員、林專員 security@cisanet.org.tw 報名截止： 2023-10-20 費用： 原價：NT 3,300 元/人 軟協會員：NT 2,800 元/人 費用含稅、教材及完課證明

企業資安實務研討會	
活動時間	**112 年 10 月 31 日(二)13:00~16:30**
活動地點	台南沙崙國科會資安暨智慧科技研發大樓(A122 第一會議室) (台南市歸仁區歸仁十三路一段 6 號)
活動網站	
活動概要	 **主辦單位：TWNIC、TWCERT/CC** 近年來，全球對於網路安全的零信任議題廣泛關注，企業組織和政府部門都對此高度重視。各界紛紛推廣新的網路安全策略，著重於零信任架構，即在允許存取之前，必須通過安全評估取得信任。主要在解決現代網路環境的複雜性，因應造成邊界不確定性的資安問題。藉由透過台灣電腦網路危機處理暨協調中心(TWCERT/CC)及專業資安講師的案例分享與專題介紹，將強化對於零信任資安的認識和防護措施，有效減少受到駭客攻擊的風險。

第 4 章、 TVN 漏洞公告

TWCERT/CC 上月份發布之嚴重程度前五資安漏洞資訊如下表：

ASUS RT-AX55、RT-AX56U_V2、RT-AC86U - Format String - 1	
TVN / CVE ID	TVN-202309007 / CVE-2023-39238
CVSS	9.8 (Critical)
影響產品	RT-AX55: 3.0.0.4.386_50460 RT-AX56U_V2: 3.0.0.4.386_50460 RT-AC86U: 3.0.0.4_386_51529
問題描述	ASUS RT-AX55、RT-AX56U_V2 與 RT-AC86U iperf 相關模組 set_iperf3_svr.cgi API 存在 format string 漏洞，該功能未對輸入的格式化字串進行適當驗證，遠端攻擊者不須權限，即可利用此漏洞進行遠端程式碼執行，對設備進行任意操作或中斷服務。
解決方法	RT-AX55: 更新至 3.0.0.4.386_51948 RT-AX56U_V2: 更新至 3.0.0.4.386_51948 RT-AC86U: 更新至 3.0.0.4.386_51915
公開日期	2023-09-05
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7354-4e654-3.html

ASUS RT-AX55、RT-AX56U_V2、RT-AC86U - Format String - 2	
TVN / CVE ID	TVN-202309008 / CVE-2023-39239
CVSS	9.8 (Critical)
影響產品	RT-AX55: 3.0.0.4.386_50460 RT-AX56U_V2: 3.0.0.4.386_50460 RT-AC86U: 3.0.0.4_386_51529

問題描述	ASUS RT-AX55、RT-AX56U_V2 與 RT-AC86U 的一般設定功能之 API 存在 format string 漏洞，該功能未對輸入的格式化字串進行適當驗證，遠端攻擊者不須權限，即可利用此漏洞進行遠端程式碼執行，對設備進行任意操作或中斷服務。
解決方法	RT-AX55: 更新至 3.0.0.4.386_51948 RT-AX56U_V2: 更新至 3.0.0.4.386_51948 RT-AC86U: 更新至 3.0.0.4.386_51915
公開日期	2023-09-05
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7355-0ce8d-3.html

ASUS RT-AX55、RT-AX56U_V2、RT-AC86U - Format String - 3	
TVN / CVE ID	TVN-202309009 / CVE-2023-39240
CVSS	9.8 (Critical)
影響產品	RT-AX55: 3.0.0.4.386_50460 RT-AX56U_V2: 3.0.0.4.386_50460 RT-AC86U: 3.0.0.4_386_51529
問題描述	ASUS RT-AX55、RT-AX56U_V2 與 RT-AC86U iperf 相關模組 set_iperf3_cli.cgi API 存在 format string 漏洞，該功能未對輸入的格式化字串進行適當驗證，遠端攻擊者不須權限，即可利用此漏洞進行遠端程式碼執行，對設備進行任意操作或中斷服務。
解決方法	RT-AX55: 更新至 3.0.0.4.386_51948 RT-AX56U_V2: 更新至 3.0.0.4.386_51948 RT-AC86U: 更新至 3.0.0.4.386_51915
公開日期	2023-09-05
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7356-021bf-3.html

ASUS RT-AC86U - Command injection vulnerability - 1	
TVN / CVE ID	TVN-202309002 / CVE-2023-38031
CVSS	8.8 (High)
影響產品	RT-AC86U: 3.0.0.4.386.51529
問題描述	ASUS RT-AC86U 之 Adaptive QoS 之網頁瀏覽歷史功能未對特殊參數作過濾，遠端攻擊者以一般使用者權限登入後，即可利用此漏洞進行 Command Injection 攻擊，執行系統任意指令，並導致阻斷系統與終止服務。
解決方法	更新至 3.0.0.4.386_51915
公開日期	2023-09-04
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7348-56989-3.html

ASUS RT-AX88U - externally-controlled format string	
TVN / CVE ID	TVN-202309010 / CVE-2023-41349
CVSS	8.8 (High)
影響產品	RT-AX88U: 3.0.0.4_388_23748(不含)以前版本
問題描述	華碩 RT-AX88U 的 Open VPN 功能存在 externally-controlled format string 漏洞。經身分驗證的遠端攻擊者，可藉由利用匯出的 OpenVPN 設定檔觸發 externally-controlled format string 漏洞，將造成 memory leakage 或是中斷服務。
解決方法	更新至 3.0.0.4_388_23748
公開日期	2023-09-15
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7371-aecf1-3.html

第 5 章、 2023 年 9 月份資安情資分享概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資，以下為各項統計數據，分別為對外資安情資分享地區統計圖及資安情資分享類型統計圖。

分享地區統計圖為本中心所接獲之資安情資分享中，針對資安情資所屬地區之分享比率，如圖 1 所示；分享類型統計圖則為本中心所接獲的資安情資分享中，各項攻擊類型之比率，如圖 2 所示。

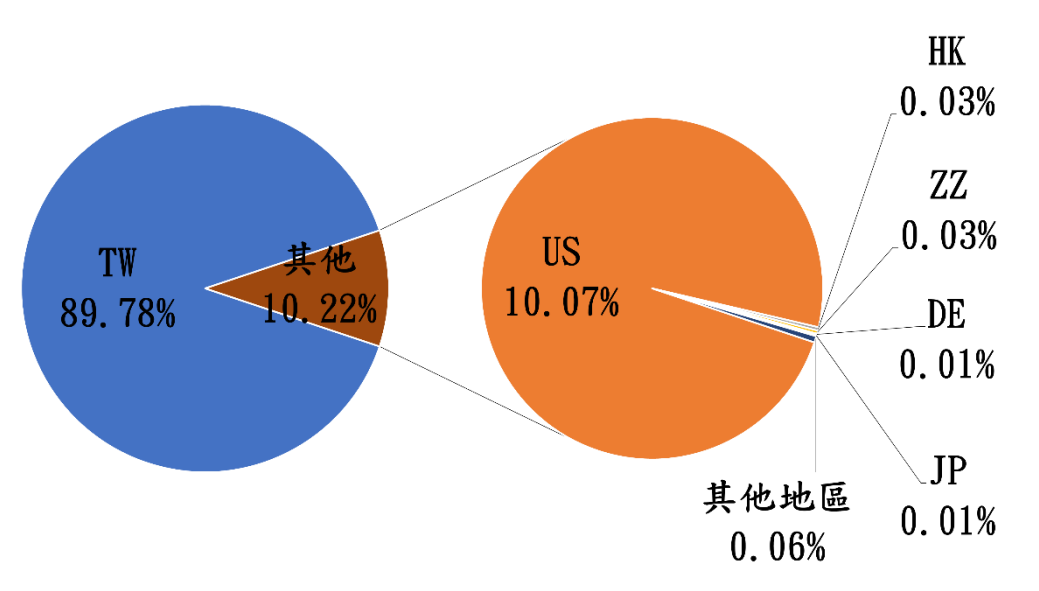


圖 1、分享地區統計圖

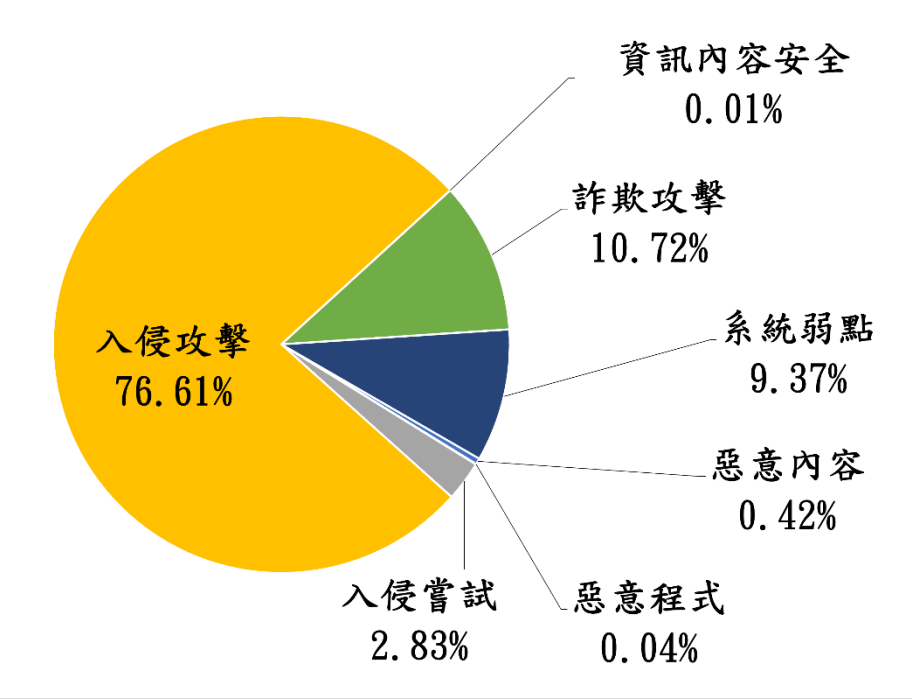

資訊內容安全
0.01%
詐欺攻擊
10.72%
系統弱點
9.37%
惡意內容
0.42%
惡意程式
0.04%
入侵嘗試
2.83%
入侵攻擊
76.61%

圖 2、分享類型統計圖

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：**2023 年 10 月 6 日**

編輯：**TWCERT/CC 團隊**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**http://twcert.pixnet.net/blog**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc/**

Instagram：**https://www.instagram.com/twcertcc/**

Twitter：**@TWCERTCC**