TWCERT/CC 資安情資電子報

2023 年 9 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

WinRAR 嚴重漏洞，開啟壓縮檔可讓駭侵者遠端執行任意程式碼

資安廠商趨勢科技旗下的資安研究團隊 Zero Day Initiatives 日前發表研究報告，指出該單位的資安研究人員，近期發現 WinRAR 內含一個嚴重漏洞，駭侵者可藉以在使用者開啟 RAR 壓縮檔時，遠端執行任意程式碼。

該漏洞的 CVE 編號為 CVE-2023-40477，問題源自對於復原檔案卷宗在處理上的錯誤，未能適當驗證用戶輸入的資訊，使得驗侵者可存取已分配緩衝區之外的記憶體。

駭侵者可將特製的 RAR 檔案傳送給攻擊目標，誘使其開啟檔案，即可利用該漏洞遠端執行任意程式碼。

CVE-2023-40477 的危險程度評分，雖然因為必須由使用者開啟檔案才能運作，所以分數僅有 7.8 分（滿分為 10 分），但是由於要誘使使用者開啟惡意檔案，在實作上並不困難，且 WinRAR 在 Windows 使用者中的普及率極高，是使用量非常大的常用工具軟體，因此這個漏洞造成的資安風險不容忽視。

發現該漏洞的 Zero Day Initiatives，在 2023 年 6 月 8 日將本漏洞通報給 WinRAR 的開發廠商 RARLAB，RARLAB 則是在近 2 個月後的 8 月 2 日推出新版的 WinRAR 6.23，解決了 CVE-2023-40477 這個漏洞。

RARLAB 這次發表的 WinRAR 6.23 版本，同時也修復了另一個由 Group-IB 發現的資安漏洞，駭侵者可利用特製的 RAR 壓縮檔讓用戶開啟錯誤的檔案。

- CVE 編號：CVE-2023-40477
- 影響產品：WinRAR 6.23 先前版本。
- 解決方案：立即更新 WinRAR 至 6.23 與後續版本。

- 資料來源：
  1. RARLAB WinRAR Recovery Volume Improper Validation of Array Index Remote Code Execution Vulnerability
  2. WinRAR 6.23 final released
  3. WinRAR flaw lets hackers run programs when you open RAR archives

第 2 章、 國內外重要資安事件

2.1、資安趨勢

Google 說明為何會有惡意軟體進入 Google Play Store 上架

Google Cloud 旗下的資安團隊 Cybersecurity Action Team，在近期發表的 2023 年資安趨勢報告「Threat Horizons: August 2023 Threat Horizons Report」中指出，愈來愈多駭侵者利用「版本置換」（Versioning）的方式，通過 Google Play Store 的上架前檢查流程並成功上架。

在這份報告中，Google 先列出 Google Cloud 2023 年第一季統計所得的雲端服務攻擊原因，其中未設定密碼或密碼不夠強，其佔比高達 54.8%；其他原因還包括資安設定錯誤（19%）、敏感 UI 或 API 曝光（11.9%）、登入資訊遭竊（7.1%）、使用軟體存有漏洞（2.4%）等。

此外，在這份報告中，Google Cloud 資安團隊也解釋 Google Play Store 中會有惡意軟體上架的原因。駭侵者多半利用一種稱為「版本置換」（Versioning）的手法，先把不含任何惡意軟體的最初版本上架到 Google Play Store 中，以通過各種資安檢查流程，成功上架到 Googel Play Store 上；待使用者下載安裝後，再以版本更新的機制，將惡意軟體酬載自第三方伺服器安裝到使用者已安裝在裝置中的 App 內。

雖然 Google 在其 Play Store 使用規範中明白規定，禁止任何軟體使用 Google Play 官方提供的更新機制以外的方式，對已下載安裝的軟體進行更新、變更或替換，也禁止自第三方伺服器下載任何可執行檔，例如 dex、JAR 等檔案，但顯然有不少 App 並未遵守這個禁令，仍會在使用者下載完沒有問題的版本後，再透過第三方伺服器安裝惡意軟體程式碼酬載。

建議 Android 使用者即使在官方 Google Play Store 中下載安裝軟體，也應在下載前先檢視其他使用者的意見回饋，如有大量負評則應避免下載。

- 資料來源：
  1. Threat Horizons
  2. Google explains how Android malware slips onto Google Play Store

2.2、新興應用資安

2.2.1、駭侵者開始訓練 AI 聊天機器人進行釣魚、惡意軟體攻擊

資安廠商 SlashNext 發現有駭侵者推出專門用於進行釣魚與惡意軟體投放攻擊的 AI 聊天機器人，分別採用最新的 ChatGPT 與 Google Bard AI 技術來訓練。

SlashNext 旗下的資安研究人員，在 7/25 發現一個自稱為 CanadianKingpin12 的駭侵者，於多個駭侵相關論壇上刊登廣告，推廣其用於進行網路詐騙、駭侵攻擊與垃圾訊息發送專用的 AI 聊天機器人 FraudGPT。

在進一步追蹤後，SlashNext 的資安研究人員證實 CanadianKingpin12 很早就開始利用在暗網上出售的各種駭侵資料集，以 ChatGPT 和 Google Bard 等大型語言模型（Large Language Model, LLM）來訓練自己的 AI 聊天機器人 DarkBART；研究人員也發現 CanadianKingpin12 也利用韓國研究人員研發的另一個大型語言模型，來訓練另一個 AI 聊天機器 DarkBERT。

根據 CanadianKingpin12 的說詞，DarkBERT 在各種運用暗網資料來訓練的 AI 駭侵工具中，可說是功能最強大的一款，可以用來進行以下攻擊：

- 發動成熟的釣魚攻擊活動，用以取得目標對象的密碼與信用卡資訊
- 執行先進的社交工程攻擊，以取得機敏資訊或目標系統的登入權限
- 利用電腦系統、軟體或網路的資安漏洞加以攻擊

- 製作並散布惡意軟體
- 利用 0-day 漏洞來獲得不法所得，或破壞目標系統

SlahNext 指出，這兩個 AI 惡意聊天機器人的開發時程都不到一個月就完成推出，由此可見 AI 的濫用，即將成為資安防護與網路犯罪令人頭痛的嚴重問題。

建議資安研究與防治單位應加強研究如何偵測並防範由 AI 執行的各種惡意攻擊手法，擁有 LLM 等先進 AI 技術的大型科技公司，亦應加強防範其工具遭到濫用於資安攻擊之上。

- 資料來源：
  1. AI-Based Cybercrime Tools WormGPT and FraudGPT Could Be The Tip of the Iceberg
  2. Cybercriminals train AI chatbots for phishing, malware attacks

2.2.2、偽冒 Flipper Zero 的詐騙網站以免費裝置誘騙用戶安裝惡意軟體

資安專業媒體 BleepingComputer 日前發現一個偽裝成 FlipperZero 官方網站的詐騙網站，以送出免費 Flipper Zero 裝置為由，誘騙受害者進入惡意網站並安裝惡意瀏覽器外掛程式。

Flipper Zero 是一個在近期引起資安研究人員與自造者高度興趣的多功能開源工具，具備相當廣泛的功能與界面，支援 RFID 模擬、多頻段無線電通訊、NFC、紅外線通訊、藍牙、乙太網路等。自該裝置推出後，許多資安人員與相關技術愛好者紛紛發表多種該裝置可使用的控制軟體，因此十分受到歡迎，出現一機難求的現象。

BleepingComupter 是在近日發現一個假冒 Flipper Zero 官方網站的詐騙活動，頻繁在 Reddit 論壇與各社群媒體上刊登廣告，宣稱只要填寫一份問卷，就能免費獲得一台原價 169 美元的 Flipper Zero。

BleepingComputer 的資安研究人員進一步發現，該詐騙網站雖然外觀十分接近 Flipper Zero 正宗官網，但網站上許多連結都代管於一個惡名昭彰的瀏覽器詐騙通知與惡意外掛程式平台 trkrspace[.]com 上。

BleepingComupter 指出，使用者如果填寫了該詐騙網站上的問卷，其個資就會被蒐集成功，包括姓名、地址、Email 等，並用於其他釣魚攻擊與詐騙攻擊活動之上；有些使用者瀏覽器還會出現假警訊，謊稱使用者的電腦發生問題、系統過載或有安全漏洞，需要安裝資安防護軟體等，藉以進一步誘騙使用者。

建議使用者對於過份好康（too good to be true）的各種廣告訊息都必須提高警覺，且勿隨意提供個人資訊。

- 資料來源：
  1. Flipper Zero
  2. Fake FlipperZero sites promise free devices after completing offer

2.2.3、多個知名加密錢包內含多個 0-day 漏洞，可能導致加密資產遭竊

資安廠商 Fireblocks 旗下的加密演算法研究團隊，在多個知名加密貨幣錢包使用的多種加密協定如 GG-18、GG-29、Lindell 17 中，發現一批稱為「BitForge」的多個 0-day 資安漏洞；駭侵者可利用這批漏洞，無需與用戶與錢包發行商互動，即可竊走錢包中的加密貨幣資產。

受到這批 BitForge 0-day 漏洞影響的加密貨幣錢包供應商，包括多家知名交易所如 Coinbase、ZenGo、Binance 等。

這批 BitForge 0-day 漏洞群中，第一個漏洞 CVE-2023-33241 存於 GG-18 和 GG-20 的「門檻式簽章協定」（Threshold signature schemes）；研究人員發現駭侵者可利用特製的訊息，在 16 位元的 Chunk 中取出金鑰分片；重覆操作 16 次後即可取得完整私鑰。

另一個存於 Lindell 17 2PC 加密協定中的 0-day 漏洞 CVE-2023-33242 也是類似的錯誤，攻擊者只要重覆 200 次操作就可以取得完整的私鑰。

Fireblocks 在報告中指出，該公司的團隊於 2023 年 5 月時發現這批 0-day 漏洞，並在第一時間通報多家加密貨幣交易所，並於近日在 BlackHat 駭侵防護研討會上公開這項研究報告。值得注意的是，在報告公開的現在，Coinbase 與 ZenGo 已修復其加密貨幣錢包中的相關漏洞，但 Binance 和其他多家加密貨幣錢包供應商，仍未能及時修復這批問題。

建議加密貨幣交易者如有利用受影響的錢包，可透過 Fireblocks 提供的網

頁，檢視受影響錢包是否已經提供更新版本，並立即加以更新。

- 資料來源：
  1. Welcome to the BitForge Status Checker
  2. New BitForge cryptocurrency wallet flaws lets hackers steal crypto

2.2.4、TP-Link 智慧燈泡內含多個漏洞，駭侵者可藉以竊得 Wi-Fi 密碼

義大利卡塔尼亞大學（Universita di Catania）與英國倫敦大學的資安研究人員，日前聯合發表研究報告；報告指出銷售量相當大的 TP-Link 智慧燈泡 Tapo L530E 與其控制用行動軟體 Tapo App，內含 4 個嚴重漏洞，駭侵者可藉以竊取使用者設定的 Wi-Fi 連線密碼。

兩所大學的資安研究人員，在進行市售 IoT 智慧聯網裝置的資安研究時，發現了這批漏洞；這些漏洞的問題分列如下：

- 其中一個漏洞可讓鄰近攻擊者取得 Tapo 系統的使用者密碼，以控制 Tapo 系列裝置
- 還有一個漏洞是硬式編碼（hard-coded）在程式碼中的共享密碼，僅使用很短的 checksum 加密，駭侵者可透過暴力試誤法取得這些密碼
- 另一個漏洞是在進行加密時缺少隨機性，因此其加密方式可預測得知
- 第四個漏洞是訊息在執行期間的有效期限長達 24 小時，使得駭侵者可以在期間內不斷重播訊息

兩所大學的研究人員，利用這四個漏洞的組合，找出多種攻擊 TP-Link Tapo 系統的概念驗證方法；其中包括利用前兩個漏洞的操作，找出使用者設定的 Wi-Fi 密碼；另一種攻擊方式是可利用第一種漏洞來發動中間人攻擊（Man-in-the-Middle Attack），用來破解裝置間溝通的 RSA 金鑰，最後也能

取得 Wi-Fi 密碼和 Tapo 本身的密碼。

研究人員在報告發表之前已通報 TP-Link，TP-Link 也在日前推出新版韌體與 App 更近，解決了這批漏洞。

建議使用各類 IoT 裝置的使用者或系統管理者，必須隨時保持這些裝置與其軟體維持在最新版本，且應在原廠發表資安修補時立即更新。

- 資料來源：
  1. Smart Bulbs can be Hacked to Hack into your Household
  2. Statement on Tapo L530 and Tapo App Vulnerabilities

2.3、國際政府組織資安資訊

2.3.1、五眼聯盟公布 2022 年遭駭最嚴重 12 個漏洞

五眼聯盟（The Five Eyes）所屬資安主管機關，近期會同美國多個資安主管單位如網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）、美國國家安全局（National Security Agency, NSA）、美國聯邦調查局（Federal Bureau of Investigation, FBI）等單位，共同發表 2022 年最常遭到用於駭侵攻擊的 12 個資安漏洞。

五眼聯盟是由美國、澳洲、加拿大、紐西蘭與英國等五個英語系國家組成的情報合作組織；其下轄的資安單位近期發表這批漏洞，意在敦促全球各公私單位，立即針對這些已造成嚴重資安風險的漏洞進行處理，以降低繼續遭到攻擊的危險。

該報告指出，近年來駭侵者更偏好使用已知的舊漏洞來發動攻擊，而非使用未公開或較新的漏洞。由於這些舊漏洞往往很長一段時間仍未受到修補，再加上有較多現成的攻擊工具與方法可以使用，因此帶來極大的資安風險。

報告也說，雖然在 2022 年中新增了近 25,000 個指派有 CVE 編號的漏洞，但名列榜上的最常遭駭漏洞中，只有 5 個是在 2022 年新發現的漏洞。

名列該份清單的漏洞如下：

- CVE-2018-13379：Fortinet SSL VPN 登入資訊外洩
- CVE-2021-34473（Proxy Shell）：Microsoft Exchange Server RCE 漏洞
- CVE-2021-31207（Proxy Shell）：Microsoft Exchange Server 資安防護功能跳過漏洞
- CVE-2021-34523（Proxy Shell）：Microsoft Exchange Server 執行權限提升漏洞
- CVE-2021-40539：Zoho ADSelfService Plus RCE/登入驗證跳過漏洞
- CVE-2021-26084：Atlassian Confluence Server/Data Center 任意程式碼執行漏洞
- CVE-2021-44228（Log4Shell）：Apache Log4j2 的 RCE 漏洞
- CVE-2022-22954：VMware Workspace ONE 的 RCE 漏洞
- CVE-2022-22960：VMware Workspace ONE 權限管理不良漏洞
- CVE-2022-1388：F5 Networks BIG-IP 驗證流程漏洞
- CVE-2022-30190：Microsoft 多種產品的 RCE 漏洞
- CVE-2022-26134：Atlassian Confluence Server/Data Center 的 RCE 漏洞

建議系統管理者需在接獲軟體系統更新通報後立即進行更新，勿留下已知漏洞，以免遭到資安攻擊而造成損失。。

- 資料來源：
  1. 2022 Top Routinely Exploited Vulnerabilities
  2. FBI, CISA, and NSA reveal top exploited vulnerabilities of 2022

2.3.2、FBI 警示：詐騙者假冒 NFT 開發人員騙取加密貨幣數位資產

美國聯邦調查局（Federal Bureau of Investigation, FBI）日前發表資安警訊，指出有詐騙集團假冒為「非同質性代幣」（Non-Fungible Token, NFT）開發人員，針對 NFT 愛好者進行各種詐騙活動，意圖竊取其加密資幣與 NFT 數位資產。

FBI 指出，這些詐騙集團以駭侵手法取得部分知名 NFT 開發人員的社群媒體帳號控制權，或是設立一個幾可亂真的假帳號，來假扮這些知名開發者的身分，藉以取信於 NFT 愛好者與投資人。

在與目標對象建立溝通管道後，這些詐騙分子就會以限時專案等誘因來誘騙目標對象，宣稱有限定參與對象的新 NFT 鑄造計畫，有極佳的投資獲利機會，邀請受害對象參加；由於詐騙集團多半會強調時限，因此受害對象往往在沒有時間進行充分查證的情形下，就受到引誘。

接著受害者會被導向到偽裝成正宗 NFT 計畫網站的惡意釣魚網站，一旦受害者輸入自己的錢包位址與存取密碼，自己擁有的加密貨幣與 NFT 等數位資產，就會遭到盜領一空。

為了防止資金流向遭到追查，這些詐騙者還會利用多種數位資產混合服務，讓執法單位難以追蹤金流，以避免遭到查緝。這也使得受害者更不容易追回損失的資金。

FBI 在這次的警訊中，沒有透露目前這波攻擊具體造成的損失金額與受

害情形，但這類案件的發生可謂層出不窮，損失金額也十分可觀。今年三月時公開的「Pig Butchering」詐騙案，損失金額就高達 20 億美元以上。

FBI 建議 NFT 愛好者在投資時，務必再三確認 NFT 開發者的身分，確認其社群媒體上的廣告真實可信；在進行相關購買時，也一定要確認網址的合法性。如果活動本身宣稱的利潤過高，就必須特別提高警覺。

- 資料來源：
  1. Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition
  2. FBI warns of scammers posing as NFT devs to steal your crypto

22.3.3、國際刑警組織逮捕竊取 4,000 萬美元的 14 名網路犯罪分子

國際刑警組織（INTERPOL）日前宣布，在一場在多個非洲國家進行的網路犯罪偵查行動中，目前已逮捕 14 名嫌犯，並破獲為數眾多的犯罪工具與不法所得。

這場行動的代號稱為「Africa Cyber Serge II」，於 2023 年正式在多達 25 個非洲國家展開偵查活動；四個月的偵辦期間，針對包括釣魚攻擊、網路勒贖、企業電子郵件駭侵（Business Email Compromise, BEC）、網路詐騙等等進行偵辦，造成的財務損失高達 4,000 萬美元。

除了逮捕網路犯罪分子之外，Africa Cyber Serge II 行動也起出大量犯罪相關工具，包括近四千台用於進行駭侵攻擊的控制伺服器、近 15,000 個用以竊取資料的 IP、近 1,500 個用於釣魚攻擊的連結與網域、近 1,000 個用於詐騙攻擊的 IP、超過 400 個其他惡意網址和僵屍網路等。

Africa Cyber Serge II 在非洲各國的執行成果，包括在喀麥隆逮捕 3 名涉及 85 萬美元網路藝術品詐騙的嫌犯、在奈及利亞逮捕一名涉嫌詐騙一名甘比亞受害者的嫌犯、在模里西斯逮捕兩名即時通訊詐財分子、在甘比亞查緝 185 個惡意 IP、在喀麥隆破獲 2 個暗網網站、在肯亞緝獲 615 台駭侵攻擊用主機。

上一次的 Africa Cyber Serge 大執法是在 2022 年 11 月發動，當時逮捕 11 名犯嫌，破獲多達 200,000 個駭侵攻擊使用的基礎設備。

- 資料來源：
  1. Cybercrime: 14 arrests, thousands of illicit cyber networks disrupted in Africa operation
  2. Interpol arrests 14 suspected cybercriminals for stealing $40 million

2.4、社群媒體資安近況

2.4.1、Google 指出 Android 各廠遲推更新，造成舊漏洞有如 0-day 一樣危險

Google 日前發表年度報告「The Ups and Downs of 0-days: A Year in Review of 0-days Exploited In-the-Wild in 2022」，在報告中除了列出在 2022 年被駭侵者積極用於攻擊的多個 0-day 漏洞之外，Google 更指出由於各 Android 設備製造廠在韌體更新推出時程的延遲，加上 Android 生態系的複雜度，由 Google 修補完成的 0-day 漏洞，駭侵者往往仍可在數月後用於攻擊。

Google 指出的這個問題，可說是 Android 系統上長年未解的老問題，主要肇因於 Google 生態系的複雜性。在該生態系，最上游的 Google 到最下游的手機製造廠，中間還有許多角色，例如品牌商（如三星、小米等）、電信業者等。這樣複雜的結構，造成即使 Google 在第一時間發表了 0-day 漏洞的修補方案，也要等品牌商或製造商針對各款手機推出韌體更新，使用者才能修補裝置上的 0-day 漏洞。

Google 說，從 Google 修補漏洞到使用者有更新版韌體可以安裝，中間往往會有好幾個月的時間間隔；而這麼長的時間差，就讓駭侵者有機可乘，可利用事實上早就可以修補的 0-day 漏洞，在很長一段時間內仍可用來發動攻擊。

舉例來說，CVE-2022-38181 是個發生在 ARM Mali CPU 的 0-day 漏洞，該漏洞於 2022 年 7 月時提報給 Android 開發團隊，並於 2022 年 10 月由

ARM 發表漏洞修補程式，但直到 2023 年 4 月時才納入 Android 2023 年 4 月的更新之中，時隔長達半年。而駭侵者早在 2022 年 11 月起，就開始利用該漏洞發動攻擊。

鑑於 Android 生態系的複雜度與較大的資安風險，Android 使用者應加強本身的資安防護措施，或考慮改用其他較安全的系統。

- 資料來源：
  1. The Ups and Downs of 0-days: A Year in Review of 0-days Exploited In-the-Wild in 2022
  2. Google: Android patch gap makes n-days as dangerous as zero-days

2.4.2、駭侵者透過假冒 Android 聊天 App 竊取 Signal、WhatsApp 用戶個資

資安廠商 CYFIRMA 旗下的資安研究人員，近期發現有 APT 駭侵團體，利用假冒的 Android 即時通訊軟體來散布惡意軟體，以竊取受害者手機中的通話記錄、文字簡訊、GPS 定位資訊與其他多種即時通訊軟體的對話內容。

CYFIRMA 指出，涉及這波攻擊行動的印度 APT 駭侵團體稱為「Bahamut」，過去主要透過 WhatsApp 來進行魚叉式釣魚攻擊，直接把惡意軟體傳送給目標對象，以進行攻擊行動。另一家資安廠商 ESET 過去也曾發現 Bahamut 使用假冒的 Android 平台 VPN 軟體來進行大規模資安攻擊。

這次 CYFIRMA 發現 Bahamut 利用一個名為「SafeChat」的假冒 Android App，在其中植入一個名為「Coverlm」的惡意軟體，用以竊取 Telegram、Signal、WhatsApp、Viber、Facebook Messenger 等多種即時通訊軟體內的對話內容；主要的攻擊對象以南亞地區的 Android 手機用戶為主。

CYFIRMA 針對 SafeChat 的分析指出，一旦用戶誤信該軟體是真實的即時通訊軟體並且安裝後，SafeChat 會要求用戶授與輔助使用權限，以自動取得存取簡訊、通訊錄、通話記錄、GPS 資訊、外接儲存裝置等權限，並進行後續的惡意軟體酬載載入與安裝。

SafeChat 甚至會要求用戶同意存取手機的電池電力最佳化子系統，這是為了阻止系統在使用者很少使用該 App 時，自動中止該 App 的執行。

建議 Android 使用者除應避免自非 Google 官方管道下載安裝 App 外，如

遇 App 要求輔助使用等權限，應立即拒絕並移除該軟體。

- 資料來源：
  1. APT Bahamut Targets Individuals with Android Malware Using Spear Messaging
  2. Hackers steal Signal, WhatsApp user data with fake Android chat app

2.4.3、大量 LinkedIn 帳號遭駭侵者發動大規模竊取攻擊

資安廠商 Cyberint 近日發表資安觀察研究報告指出，全球最大求職求才社群服務 LinkedIn，日前發生大規模帳號遭攻擊事件，大量帳號因而遭到竊取，或被系統認定為不安全帳號而遭鎖定。

Cyberint 近期觀察到在包括 X（即改名後的 Twitter）、Reddit 討論區與 Microsoft forum 等處，有許多使用者抱怨其 LinkedIn 帳號發生問題；許多帳號因遭到攻擊而被 LinkedIn 鎖定而無法使用，甚至還有不少帳號直接被竊。

這些帳號遭到攻擊的使用者也在上述社群頻道中抱怨，LinkedIn 的客戶服務系統不但未能及時解決使用者的帳號問題，甚至對用戶的反應沒有任何回應。

Cyberint 的資安研究人員指出，LinkedIn 的客服系統最近的反應遲緩，顯示該服務可能面臨較平時高出甚多的客服需求，以致客服系統與人員難以負荷。

駭侵者很可能是利用暴力試誤法，或使用已洩漏的登入資訊，來竊取使用者的 LinkedIn 帳號。有不少使用者的 LinkedIn 帳號，其登入密碼和 Email 遭到竄改，以致無法登入。

Cyberint 說，駭侵者甚至會在竊得帳號後開啟二階段登入驗證，導致使用者要取回帳號存取權的難度進一步提高。 目前已有一部分 LinkedIn 帳號遭竊的用戶，遭到駭侵者要求支付小額贖款；駭侵者威脅如果拒付贖款，帳號

即將遭到刪除。

LinkedIn 的帳號經常用來作為進一步發動社交攻擊的工具，因此在駭侵者眼中是相當有價值的攻擊目標。

建議 LinkedIn 使用者應加強帳號密碼的保護，例如開啟二階段登入驗證、不使用與其他服務相同的密碼、使用強式密碼等等。

- 資料來源：
  1. LinkedIn Accounts Under Attack
  2. LinkedIn accounts hacked in widespread hijacking campaign

2.4.4、Discord 通知用戶資料因駭侵攻擊而外洩

十分受全球網友歡迎的社群聊天室服務 Discord，日前開始發送 email 通知部分用戶，因該平台先前發生的駭侵事故，導致這批用戶的個人可識別資訊（personally identifiable information, PII）外洩。

該次駭侵事件發生在 2023 年 3 月 29 日，起因是負責承包 Discord 平台客戶服務工作的第三方廠商一名工作人員，疑似遭到社交攻擊，導致駭侵者取得其工作用登入資訊，並藉以取得 Discord 平台部分系統的使用權限。

駭侵者竊得的資料，包括客服系統中的支援工單佇列、用戶的 email 地址、與客服人員溝通的訊息記錄，以及支援工單中附件的檔案內容。

Discord 表示在發現系統遭到不當存取，且證實資料遭竊後，該公司立即停用遭駭人員帳號的相關權限，清查後發現約有 180 名使用者的個人機敏資料遭到竊取。

Discord 在新聞稿中指出，目前證實有一名位於美國緬因州的使用者，其個人姓名、駕駛執照、州民證號碼等資訊遭到外洩。

另外，在先前有一家第三方、非官方的 Discord 邀請服務 Discord.io，在遭到駭侵攻擊並發生大量資料外洩後停止服務；資料遭到外洩的該服務使用者據傳多達 760,000 人。

Discord.io 被竊取的使用者資訊，據傳也在一個新成立的駭侵討論區 Breached 上出售，駭侵者還公開了 4 名使用者的資訊，以佐證該批資料的真

實性。遭竊的資料欄位包括使用者名稱、email 地址、帳單地址（部分使用者）、已加密的密碼 hash、對應的 Discord ID 等。

鑑於第三方服務業者人員遭社交攻擊等方式，導致平台系統遭到駭侵的案例層出不窮，建議各平台業者加強第三方業者的資安認證與人員教育訓練，並將核心系統與資料進行必要的隔離保護。

- 資料來源：
  1. Data Breach Notifications
  2. The data of 760,000 Discord.io users was put up for sale on the darknet

2.5、行動裝置資安訊息

2.5.1、數千種 Android 惡意軟體 APK 使用特殊壓縮方式逃避分析

資安廠商 Joe Security 與 Zimperium 近期分析發現，有數千種 Android 惡意軟體的 APK 安裝檔，採用非正規的壓縮方式，能夠成功避開多種防毒防駭工具的偵測；而且採用這種方式的惡意 Android APK 數量持續增加。

這些惡意軟體 APK 檔採用的壓縮方式，許多並未在 Android 系統中提供支援，也有一部分是非公開的壓縮演算法，或是經過大幅改寫，以致於無法使用公用解壓縮方式解壓。

據 Zimperium 的研究指出，市面上有至少 3,300 種 APK 使用這類特殊的壓縮方式，來規避防毒防駭機制的掃瞄；雖然許多 APK 都因此容易發生不穩定而當機的狀況，但 Zimperium 還是發現至少有 71 種惡意 APK 可在 Android OS 9 (API28) 版本上正常運作。

研究人員也表示，使用作業系統不支援或未知的壓縮演算法的 APK，無法在 Andoird 8 或先前版本上執行，但卻可在 Android 9 與後續版本上執行。另外，採用這種非正規的壓縮方式，駭侵者還可以使用超過 256 字元以上的檔名，這可造成許多惡意軟體分析工具無法執行。

研究人員指出，利用這種非正規的方式來壓縮 APK 檔，就能有效避開市面上多種 Android 平台上的防毒防駭軟體的靜態偵測機制，也能有效延緩資安廠商與研究人員分析惡意軟體並推出解決方案的速度。

研究人員也說，目前這些變造壓縮方式的 Android APK 檔，均未在 Google Play Store 中上架，但很可能出現在第三方的 App Store 中。

建議 Android 用戶避免下載安裝來路不明、非出自官方 Google Play Store 的 APK 檔案。

- 資料來源：
  1. Over 3,000 Android Malware Samples Using Multiple Techniques to Bypass Detection
  2. Thousands of Android APKs use compression trick to thwart analysis

2.6、軟體系統資安議題

2.6.1、Tesla 車內資訊娛樂系統可遭破解並解鎖付費專屬功能

德國柏林科技大學（Technical University of Berlin）的資安研究人員，日前表研究報告，指出研究人員發展出一種破解 Tesla 車內資訊娛樂系統（Infotainment systems）的方法，可以破解 Telsa 對某些付費專屬軟體的限制。

Tesla 車內配備的資訊娛樂系統，採用由晶片設計大廠 AMD 生產製造的 AMD Zen 1 CPU 作為主要處理器；研究人員利用逆向工程技術，追蹤該系統的啟動流程，並且找到該晶片系統的「越獄」（jailbreak）方法。

研究團隊表示，在越獄後，研究人員即可自由啟用通常必須付費才能使用的 Tesla 車內進階功能，例如電熱椅或更凌厲的加速動力。

此外，由於研究人員能夠以這種破解法取得該資訊娛樂系統的 root 權限，因此也能夠竊得車主的多種機敏個人資料，包括車主個人資訊、通訊錄內容、行事曆項目、電話通聯紀錄、Spotify 與 Gmail 連線階段的 cookie、Wi-Fi 密碼、曾造訪過的地點等多項資訊。

研究人員也說，這個破解方式也能夠讓車輛在尚未支援的地區行駛，並且讓車主可以自行進行車輛維修、系統修改等。

研究團隊在找到破解的概念驗證方法後，隨即通報 Tesla 原廠；Tesla 原廠在稍後發表聲明，指出該團隊用以破解以啟動電熱椅的方法，僅適用於舊

版 Tesla 韌體，新版韌體已加強安全簽署流程；然而研究團隊指出該攻擊方法照樣可適用於目前推出的最新版韌體。

此外，有部分媒體在相關報導中指出，可利用該破解法啟用「完全自動駕駛」（Full Self-Driving, FSD）功能，但該團隊指出報導是錯誤的，並無法使用該破解方式啟用 FSD。

建議智慧車輛車主對此類破解消息應謹慎處理，避免自行套用，以免影響行車安全。

- 資料來源：
  1. Jailbreaking an Electric Vehicle in 2023 or What It Means to Hotwire Tesla's x86-Based Seat Heater
  2. Tesla infotainment jailbreak unlocks paid features, extracts secrets

2.6.2、MalDoc in PDF 利用嵌入 PDF 的惡意 Word 檔發動攻擊

日本電腦網路危機處理暨協調中心 (JPCERT/CC) 日前發布資安警訊，指出一種全新駭侵攻擊方式；駭侵者利用嵌入在 PDF 檔中的惡意 Word 檔案來逃避防毒防駭軟體的偵測，成功發動攻擊。

JPCERT/CC 是在 2023 年 7 月開始觀察到利用這種技術發動的資安攻擊案例。該單位分享了一個樣本檔案，是一種集多種檔案格式於一身的特殊檔案，可以同時使用不同的軟體來開啟；多數的防毒防駭軟體，在對該樣本檔案進行掃瞄偵測時，會把該檔案當做是 PDF 檔，但該樣本檔同時也可以由 Microsoft Word 來開啟。

JPCERT/CC 指出，該樣本檔一旦由受害者以 Microsoft Word 開啟，即會執行其內含的 VBS 巨集，並且下載一個含有惡意軟體的 MSI 檔案，安裝在受害者的 Windows 系統中。

資安專家指出，駭侵者經常利用這種多合一格式檔案來放置內含 VBS 惡意巨集程式碼的 Word 檔案，由於掃毒軟體會把這種檔案當成相對無害的 PDF 檔，因此往往能成功避開系統上安裝的資安防護機制。

資安專家分析指出，雖然 JPCERT/CC 沒有進一步公開樣本檔內含的惡意軟體攻擊行為與方式，但一般來說，用戶可以在 Microsoft Office 相關設定中，停用巨集的自動執行功能，這樣就能夠阻止這類多合一格式惡意檔案的執行。

此外，還是有一些如 OLEVBA 之類的資安防護軟體，可以偵測到這類多合一格式的惡意檔案內含的惡意程式碼。

建議使用者避免開啟來路不明的任何檔案，系統管理者也應提防這類攻擊，在布署軟體時強制關閉 Office 巨集的自動執行。

- 資料來源：
  1. MalDoc in PDF - Detection bypass by embedding a malicious Word file into a PDF file –
  2. MalDoc in PDFs: Hiding malicious Word docs in PDF files

2.7、軟硬體漏洞資訊

2.7.1、全新發現的 Collide+Power 旁路攻擊，影響幾乎所有 CPU 款式

奧地利格拉茨科技大學（Graz University of Technology）的研究團隊，近日發現各廠牌推出的中央處理器（Central Processing Unit, CPU）中，存有一個共同的漏洞「Collide+Power」，可讓駭侵者以特殊方式竊得 CPU 內傳輸的資料。

根據格拉茨科技大學團隊的報告指出，該漏洞的實作方式，是駭侵者可藉由駭侵者對 CPU 發出的資料集，在 CPU 中與其他應用程式送出的資料發生「對撞」（collision）時，改寫先前存在 CPU 快取記憶體中儲存的資料時，來測量 CPU 的耗電量變化，因而取得某些機敏資訊。

研究人員指出，受此 Collide+Power 漏洞影響的 CPU 款式可能十分廣泛，包括 Intel、AMD 或基於 ARM 架構設計的 CPU 都可能含此漏洞；雖然目前無法一一確認實際含有該漏洞的 CPU 型號有哪些，但研究人員假設所有型式的 CPU 都含有此漏洞。

該漏洞也已經提報為 CVE-2023-20583，但其 CVSS 危險程度評分僅有 4.7 分（滿分為 10 分），危險程度並不高；對此研究人員指出主要是因為 Collide+Power 攻擊取得的資料精確度並不高，而且必須以繁雜的方式進行實體接線，並進行複雜的計算分析，才能測量到 CPU 耗電量的變化，因此包括研究人員與 AMD 公司，都認為終端用戶不太容易受到駭侵者以此方式進行

攻擊。

研究人員也表示，當代 CPU 的設計中，不容易避免資料碰撞的問題發生；即使發現 Collide+Power 理論上可使用資料碰撞問題來竊取資料，但因此而大幅修改 CPU 的設計方式是不切實際的；比較合理的方式是阻止駭侵者有機會接觸電腦設備，以測量 CPU 的用電量變化才對。

- CVE 編號：CVE-2023-20583
- 影響產品(版本)：各廠牌 CPU 都可能有此問題，但攻擊實作困難，一般用戶無需擔憂。
- 解決方案：建議妥善管制重要設備的存取權限，避免駭侵者有機會接觸電腦實體，並裝設測量設備。

- 資料來源：
  1. Collide+Power
  2. Software based Power Side Channel on AMD CPUs

2.7.2、Microsoft 推出 2023 年 8 月 Patch Tuesday 每月例行更新修補包

Microsoft 日前推出 2023 年 8 月例行資安更新修補包「Patch Tuesday」，共修復 87 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 87 個，較上個月（2023 年 7 月）的 132 個資安漏洞少了很多；而在這 87 個漏洞中，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 23 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：

- 權限提升漏洞：18 個；
- 資安防護功能略過漏洞：3 個；
- 遠端執行任意程式碼漏洞：23 個；
- 資訊洩露漏洞：10 個；
- 服務阻斷（Denial of Service）漏洞：8 個；
- 假冒詐騙漏洞：12 個；
- Edge -Chromium 漏洞：12 個。

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

第一個是 CVE 編號為 CVE-2023-36884 的 Microsoft Office Defense 遠端執行任意程式碼漏洞；該漏洞存可讓駭侵者跳過先前針對該漏洞發表過的資安更新，再次利用此漏洞來遠端執行任意程式碼。Microsoft 也指出該漏洞已遭一個名為 RomCom 的駭侵團體大規模用於攻擊。

第二個值得注意的漏洞是 CVE-2023-38180，是存於 Microsoft .Net 與 Visual Studio 的服務阻斷漏洞（Denial of Service, DoS）；不過 Microsoft 並未公開說明這個漏洞是否已遭用於攻擊，也沒有分享該漏洞的細節。。

- CVE 編號：CVE-2023-36684、CVE-2023-38180
- 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 用戶盡速依照指示，套用 Patch Tuesday 與不定期發表的資安更新，以避免駭侵者利用未及更新的漏洞發動攻擊。

- 資料來源：
  1. Microsoft Office Defense in Depth Update
  2. .NET and Visual Studio Denial of Service Vulnerability
  3. Microsoft August 2023 Patch Tuesday warns of 2 zero-days, 87 flaws

2.7.3、WordPress 外掛程式 Jupiter X Core 內含嚴重漏洞，可導致帳號被盜

資安廠商 Patchstack 旗下的資安研究分析人員，日前發現廣受歡迎的 WordPress 外掛程式 Jupiter X，內含兩個嚴重漏洞 CVE-2023-38388 和 CVE-2023-38389，可導致使用者的帳號遭竊，網站遭不當上傳檔案。

Jupiter X Core 是一個十分簡單好用的視覺化編輯器，屬於 Jupiter X 佈景主題的一部分，可以讓使用者快速設計好 WordPress 與 WooCommerce 網站的外觀；目前使用該佈景主題的 WordPress 與 WooCommerce 網站約有 170,000 個。

Patchstack 的報告中指出，第一個漏洞 CVE-2023-38388 可讓駭侵者未經登入驗證即上傳任意檔案到 WordPress 網站中，可用以在伺服器上執行任意程式碼；該漏洞的 CVSS 危險程度評分高達 9.0 分（滿分為 10 分），所有 Jupiter X Core 3.3.5 之前版本都含有這個漏洞。

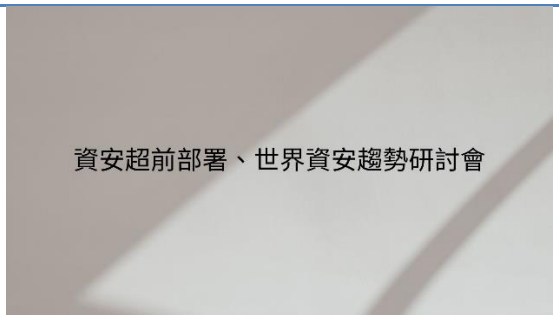
至於第二個漏洞 CVE-2023-30389 則可讓未經授權的駭侵者，只要持有任何 WordPress 帳號登入時使用的 Email 地址，即可竊取該帳號的登入權限。該漏洞的 CVSS 危險程度評分更高達 9.8 分，影響所有 Jupiter X Core 3.3.8 之前的版本。

截至目前為止，資安廠商尚未發現有駭侵者利用這兩個漏洞大規模發動攻擊的跡象；而針對這兩個漏洞，開發廠商也已經緊急推出新版 Jupiter X Core 3.4.3，順利修復漏洞。

- CVE 編號：CVE-2023-38388、CVE-2023-38389
- 影響產品(版本)：
- 解決方案：正在使用 Jupiter X 佈景主題的使用者，應立即將其中的 Jupiter Core X 更新到最新 3.4.3 版本，以免遭駭侵者利用已知漏洞發動攻擊。

- 資料來源：
  1. Critical Vulnerabilities Patched in Jupiter X Core Plugin
  2. Jupiter X Core WordPress plugin could let hackers hijack sites

第 3 章、 資安研討會及活動

資安超前部署、世界資安趨勢研討會	
活動時間	112 年 9 月 12 日(星期二)【上午場】9 時-12 時/【下午場】13 時-16 時
活動地點	台大醫院國際會議中心 301 廳（台北市中正區徐州路 2 號）
活動網站	https://www.informationsecurity.com.tw/seminar/2023_ssdlc/
活動概要	 **主辦單位：財團法人電信技術中心** 財團法人電信技術中心在數位發展部的支持下執行「5G 及物聯網資安防護-健全電信資安防護設備建置」計畫，為確保我國 5G 網路之安全、具強韌及可信賴，建立國家級通訊領域軟體安全實驗室並導入國際組織承認的軟體檢測認驗證機制，有助於主管機關與業界建立安全軟體整合開發共通性的安全認知，協助業者縮短軟體產品正式介接系統前的安全認證時程，提升軟體安全品質，並逐步厚植國內資安防護能量。 為協助我國 5G 及物聯網相關軟體資訊安全提升防護能力，特舉辦此次研討會議針對軟體資訊安全的世界趨勢進行討論，邀請國際專家針對國際物聯網資安發展的趨勢及 SBOM 強化軟體供應鏈進行專題報告，並報告建構安全軟體開發流程的機制，從軟體設計著眼找出軟體開發流程提升資安防護的機制，藉由財團法人電信技術中心提供自助式的軟體檢測及深度網站弱掃服務，可協助業者找出更多的軟體弱點及漏洞威脅，進而修復以強化資安能力。本次活動亦闡述無人機的資安議題、5G xAPP 資安防護等領域資通安全威脅及防護方式，以協助

	我國 5G 及物聯網相關軟體資訊安全的防護能力提升。 活動洽詢：02-2577-4249#970、913、305 邀請對象：本研討會免費報名，歡迎物聯網系統整合商/資訊服務商/資安業者/網通設備商/醫療資訊業者之開發人員、專案人員及採購人員踴躍參與! ※ 主辦單位保留變更議程順序、內容及相關事項之權利，不再另行通知。

【資安課程】SSDLC 安全軟體開發實務課程 (初階班、進階班)｜ACW SOUTH 數位產業署沙崙資安服務基地	
活動時間	**初階班：112 年 9 月 20 日(三) 9:00-16:30** **進階班：112 年 9 月 27 日(三) 9:00-16:30**
活動地點	**資安暨智慧科技研發大樓-A122 第一會議室** **(臺南市歸仁區歸仁十三路一段 6 號)**
活動網站	**https://ievents.iii.org.tw/EventS.aspx?t=0&id=2212**
活動概要	 **主辦單位：數位發展部數位產業署** 軟體的安全性無疑是資訊安全中極重要的一環，無論是企業內部團隊或委外開發資訊軟體，皆應注重程式的安全性，才有可能防止資料或程式碼遭受到威脅，進而降低資安風險。 #ACW_SOUTH 沙崙資安服務基地 將於 2023. 9. 20(三)及 9. 27(三)開設『SSDLC 安全軟體開發實務課程 (初階班、進階班)』。透過 2 堂課程，讓您從需求、設計、開發、測試、佈署和維運等各個環節，掌握 SSDLC(安全軟體開發生命週期)這套方法論，並協助產業提升資安能量。

【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

史諾登事件十週年，我們仍在找尋隱私與安全之平衡點	
活動時間	**2023 年 09 月 20 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/20230920/**
活動概要	 **主辦單位：TWNIC、NII、TWIGF** 史諾登在 2013 年公開大批美國國安局機密文件，揭露美國政府長期廣泛監控他國及本國政治領袖乃至平民百姓，引發全球關注。他所揭露的文件產生了巨大且持久的影響力，不只是讓全球重新檢視全面監控和資料隱私間的關係，也加速了加密技術的使用。 在網際網路生態系統中，技術社群因史諾登事件開始強化並推動各種加密協定。網際網路工程任務組（IETF）於 2014 年發布 RFC7258，主張「侵入是監控是一種攻擊」。Let’ s Encrypt 在 2015 開始發放免費憑證，鼓勵網站採用加密協定。以此為始，各種保護 DNS 訊務、網路瀏覽紀錄、電子郵件內容隱私的加密技術快速進展，「保護個人隱私」，至少以技術而言，成為對基本網路服務的基本期待。 然而，保護個人隱私的努力從來不缺乏反制力量。除了「監控資本主義」的商業力量，國家政府始終以保護人民安全為名，主張檢視加密內容的權力。即將正式成為法律的英國線上安全法案（Online Safety Bill）要求科技公司，包括社群媒體平臺及端對端加密通訊軟體，監控掃描自家平臺以即時發現並向執法單位通報兒少性虐待內容。另一方面，歐盟也正在考慮制訂類似法案。

	誠如最近一篇回顧史諾登事件後 10 年的 IETF 草稿所言，即使是人權也可能互相衝突，保護了一種就只能犧牲另一種。如何在法制、市場、網路集中化等各種壓力下，仍維持隱私與安全之間的平衡，是需要齊聚政府、企業、公民社會和技術社群等利害關係方討論的經典議題。

【資安學院-國際證照班】10/2-10/4、10/12-10/13 ISO 27001：2022 資訊安全管理系統主導稽核員訓練課程	
活動時間	**10/2-10/4、10/12-10/13 (共五日 40hr，須全程參與)**
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/3963**
活動概要	 **主辦單位：中華民國資訊軟體協會** ISO 27001 目前已是國際資訊安全管理的準則及規範，更是各國企業組織展現其在資訊安全管理能力的最佳證明！ISO/IEC 27001 於 2022 年 10 月 25 日正式頒佈新版標準，除小幅更動以符合新的 ISO 調和結構，更在安全控制措施面進行諸多新增與調整，以滿足企業組織所面臨的資安挑戰。取得「ISO 27001 資訊安全管理系統主導稽核員專業證照」，將代表個人在資安管理上建置與稽核的專業能力受到肯定，所學將可實際運用在資訊安全領域的技術職、管理職，將對個人工作升遷、機會尋找、生涯發展有所助益；除強化個人競爭例外，更有助於提升企業組織之資安能量！ 費用： 原價：NT 56,000 元/人 軟協會員/公家機關：NT 48,000 元/人 四人團報價：NT 51,000 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： 2023-09-22

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：

一等一科技 U-Office Force - Arbitrary File Upload	
TVN / CVE ID	TVN-202308003 / CVE-2023-32757
CVSS	9.8 (Critical)
影響產品	U-Office Force: 20.0.7668D
問題描述	一等一科技 U-Office Force 的檔案上傳功能未對上傳檔案做檢查限制，主機啟用網頁服務並可從外部存取 UOF 應用程式的條件下，不須登入的遠端攻擊者可以上傳任意檔案，進而執行任意程式碼或中斷系統服務。
解決方法	更新版本至 24.50SP1 或更新版本
公開日期	2023-08-25
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7330-94442-3.html

視博網訊 SpotCam FHD 2- Use of Hard-coded Cryptographic Key - 1	
TVN / CVE ID	TVN-202308004 / CVE-2023-38024
CVSS	9.8 (Critical)
影響產品	SpotCam FHD 2: 1.0036
問題描述	SpotCam FHD 2 的隱藏 Telnet 功能使用 hard-coded Telnet 帳密，遠端攻擊者可利用此漏洞登入系統，進而取得遠端主機的管理存取權。
解決方法	更新 firmware 版本至 1.0039 或更新版本
公開日期	2023-08-25
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7331-9099e-3.html

視博網訊 SpotCam FHD 2 - Use of Hard-coded Cryptographic Key - 2	
TVN / CVE ID	TVN-202308006 / CVE-2023-38026
CVSS	9.8 (Critical)
影響產品	SpotCam FHD 2: 1.0036
問題描述	SpotCam FHD 2 的使用 hard-coded uBoot 帳密，遠端攻擊者可利用此漏洞登入系統，進而取得遠端主機的管理存取權。
解決方法	更新 firmware 版本至 1.0039 或更新版本
公開日期	2023-08-25
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7333-972ca-3.html**

視博網訊 SpotCam FHD 2 - Command Injection	
TVN / CVE ID	TVN-202308005 / CVE-2023-38025
CVSS	9.8 (Critical)
影響產品	SpotCam FHD 2: 1.0036
問題描述	SpotCam FHD 2 的 隱藏 Telnet 功能存在 command Injecction 漏洞。遠端攻擊者不須權限，即可利用此漏洞進行 Command Injection 攻擊，執行任意系統指令，進而對系統進行控制，並中斷服務。
解決方法	更新 firmware 版本至 1.0039 或更新版本
公開日期	2023-08-25
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7332-ee011-3.html**

Saho 商合行 ADM100 & ADM-100FP - Arbitrary File Upload	
TVN / CVE ID	TVN-202308009 / CVE-2023-38029
CVSS	9.8 (Critical)
影響產品	ADM-100: 0.0.4.0, 0.0.4.3, 0.0.4.6, 0.0.4.8, Q20100602, T17041702, T18051803, T190 ADM-100FP: Q20100602, T17041702, T18051803, T190
問題描述	Saho 商合行 ADM100 與 ADM-100FP 的檔案上傳功能未過濾特殊字元與驗證檔案類型，遠端攻擊者不須權限，即可上傳並執行任意類型的檔案，對系統進行任意操作或中斷服務。
解決方法	請聯繫商合行詢問相關修補建議
公開日期	2023-08-25
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7336-35a94-3.html**

第 5 章、 2023 年 8 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。

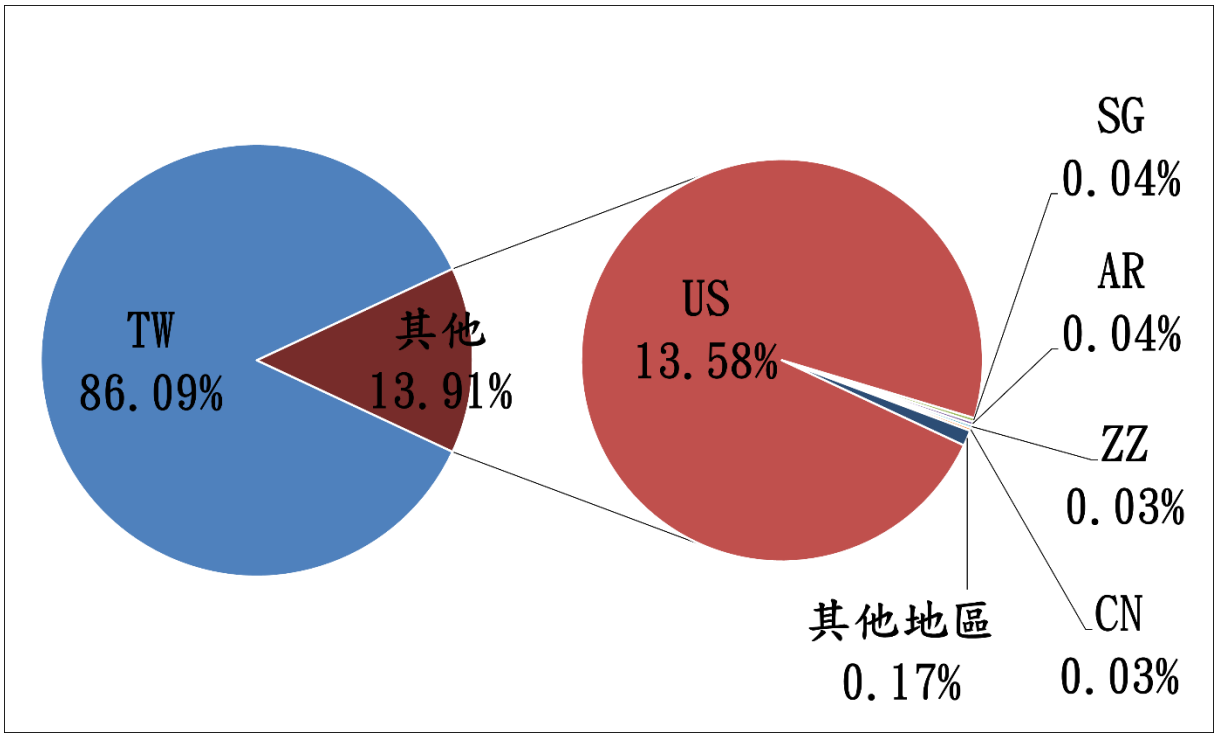


圖 1、分享地區統計圖

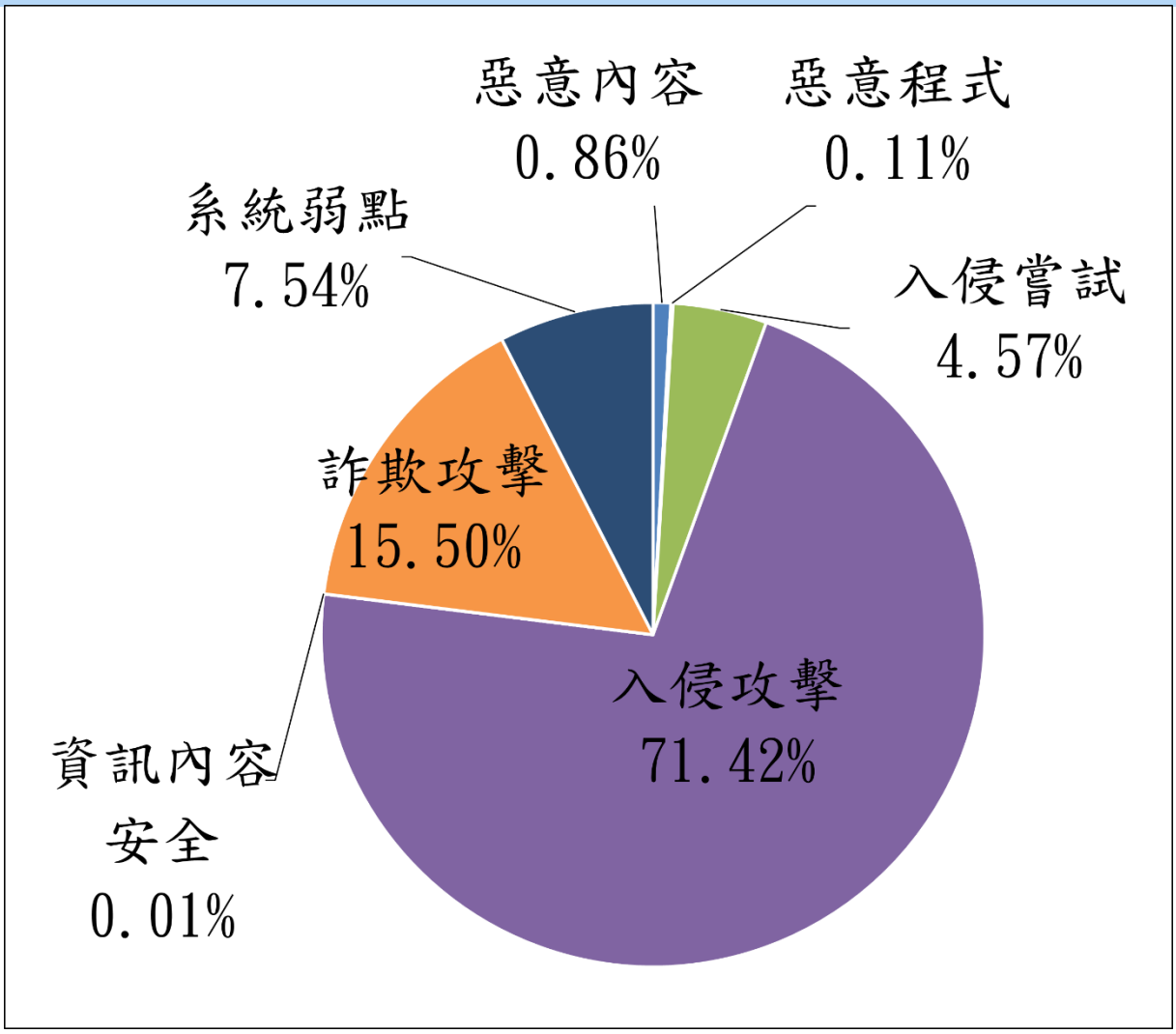

惡意內容
0.86%
惡意程式
0.11%
系統弱點
7.54%
入侵嘗試
4.57%
詐欺攻擊
15.50%
入侵攻擊
71.42%
資訊內容
安全
0.01%

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 9 月 8 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**