TWCERT/CC 資安情資電子報

2023 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：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、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 1
資安專家發現數百個 Python 程式庫含有惡意程式碼，會竊取機敏資訊 1
第 2 章、 國內外重要資安事件 3
2.1、 資安趨勢 3
統計：過半醫療機構無力對抗 BEC 駭侵攻擊 3
2.2、 新興應用資安 5
2.2.1、 駭侵新手法：將惡意程式碼藏身於區塊鏈內，更加難以偵測並下架 5
2.2.2、 詐騙集團利用以巴戰爭人道救援騙取加密貨幣捐款 7
2.3、 國際政府組織資安資訊 9
2.3.1、 美國資安主管機關揭露前 10 大資安錯誤設定 9
2.3.2、 美國資安主管機關公布勒贖團體經常攻擊的漏洞與錯誤設定 11
2.3.3、 奧地利警方破獲網路電視影片盜播網 13
2.3.4、 印度發動全國執法行動，查緝網路與加密貨幣詐騙分子 15
2.4、 社群媒體資安近況 17
2.4.1、 惡意軟體 DarkGate 透過遭駭 Skype 與 Teams 帳號散布 17
2.4.2、 駭侵團體假冒 Cosair 在 LinkedIn 上徵才，藉機散布惡意軟體 19
2.5、 行動裝置資安訊息 21
2.5.1、 Android 10 月更新包修復 54 個漏洞，部分已遭用於駭侵攻擊 21
2.5.2、 Gooogle Play Store 推出惡意軟體即時掃瞄功能 23
2.5.3、 資安專家發現 Android 木馬惡意軟體，可盜錄通話內容 25
2.5.4、 多個 Android 惡意軟體上架 Google Play Store，下載達 200 萬次 27
2.6、 軟體系統資安議題 29
Microsoft 緊急推出 Edge、Teams 更新，修復 2 個開源組件中的 0-day 漏洞 29
2.7、 軟硬體漏洞資訊 31
2.7.1、 多款路由器遭植入 Mirai DDoS 僵屍網路變種惡意軟體 31
2.7.2、 Google 修復已遭用於攻擊的 Chrome 0-day 漏洞 33
2.7.3、 Microsoft 推出 2023 年 10 月 Patch Tuesday 每月例行更新修補包，共修

復 104 個資安漏洞，內含 3 個 0-day 漏洞 35
第 3 章、 資安研討會及活動 37
第 4 章、 2023 年 10 月份資安情資分享概況 43

第 1 章、 封面故事

資安專家發現數百個 Python 程式庫含有惡意程式碼，會竊取機敏資訊

資安廠商 Checkmarkx 旗下的資安研究人員，近期發現一波惡意攻擊活動，駭侵者在數百種開源 Python 程式庫中植入惡意程式碼，用以竊取機敏資訊；目前這些惡意程式庫的下載次數已達 75,000 次。

Checkmarx 的供應鏈資安團隊，發現這波攻擊行動已持續近半年，在多達 272 個不同的開源 Python 程式庫中植入了可用以竊取各種機敏資訊的惡意程式碼，而駭侵者也利用各種混淆手法來掩飾這些惡意程式碼不被資安防護工具發現。

研究人員是從 2023 年 4 月開始發現 Python 生態系中出現這種攻擊手法，以一支名為「_init_py」的 Python 程式為例，一旦執行後，就會在受害系統中竊取下列資訊：

- 系統上執行的防毒防駭工具相關資訊；
- 系統執行工作列表、Wi-Fi 密碼、系統資訊；
- 瀏覽器中儲存的登入帳密、瀏覽記錄、付款資訊等；
- Atomic、Exodus 等加密貨幣錢包 app 資料；
- Discord 相關資訊、電話號碼、email 地址、nitro 狀態；
- Minecraft 和 Roblox 用戶資料。

該惡意軟體也會監控使用者的剪貼簿，竊取用戶複製的加密貨幣錢包位址，並以駭侵者控制的錢包位址加以替換，以竊取用戶的加密貨幣轉帳資金。

另外 Checkmarx 也發現有惡意軟體會替換掉加密貨幣錢包軟體 Exodus 的核心檔案，不但可以閃避系統的資安檢查程序，還可以竊取用戶的相關資料。像這樣可操弄應用軟體的惡意程式碼也不在少數。

為避免這類供應鏈攻擊有效發生，建議程式開發者避免自不明第三方平台下載開源套件，應從開發者官方網站下載，且應檢查套件與正版源碼的一致性，再行使用於軟體中。

- 資料來源：
  1. The evolutionary tale of a persistent Python threat
  2. Hundreds of malicious Python packages found stealing sensitive data

第 2 章、 國內外重要資安事件

2.1、資安趨勢

統計：過半醫療機構無力對抗 BEC 駭侵攻擊

資安廠商 Proorfpoint 與 Ponemon Institute 日前聯合發表一份針對醫療保健單位的資安研究調查報告「The Cost and Impact on Patient Safety and Care」；報告指出，僅有 45% 的醫療單位具備防護 BEC 與供應鏈攻擊的能力，且 64% 醫事單位在近兩年內平均遭到 4 次供應鏈攻擊。

這份調查報告向 17,805 名負責醫事單位資安或 IT 權責人員發出問卷，有效填答問卷有 653 份，調查對象包括各大公私立醫療院所、醫療健康保險業者、生物科技相關業者、藥事單位等。

調查報告揭露的重要數字如下：

- 88% 的受訪者曾在過去 12 個月內至少遭到 1 次駭侵攻擊；
- 平均遭到的資安攻擊次數達 40 次；
- 54% 受訪者在過去 2 年內平均遭到 4 次勒贖攻擊；
- 54% 受訪者在過去 2 年內平均遭到 5 次 BEC 攻擊；
- 64% 受訪者在過去 2 年內平均遭到 6 次供應鏈攻擊；
- 63% 受訪者在過去 2 年內其雲端平均遭到 21 次駭侵攻擊；

- 53% 受訪者表示遭到攻擊最多的雲端服務為專案管理與遠距會議系統；
- 高達 100% 受訪者都曾發生至少 1 次造成醫療資料被竊或損失的攻擊；
- 各受訪者平均有 19 次攻擊事件會造成資料損失；
- 47% 受訪者表示院內員工不了解其透過 email 分享的資料會有隱私與機密問題。

另外有 61% 受訪者認為自攜設備（BYOD）的使用會帶來更多資安隱患，比例較去（2022）年提高 34%；而對 BEC/冒名釣魚攻擊的憂慮，也自前一年的 46% 提高到今年達 62%。

建議各醫療單位除應強化自身的資安防護能力外，對從業人員的資安教育訓練亦應大幅加強。

- 資料來源：
  1. Patient care threatened by ever-increasing cyberattacks
  2. THE COST AND IMPACT ON PATIENT SAFETY AND CARE

2.2、新興應用資安

2.2.1、駭侵新手法：將惡意程式碼藏身於區塊鏈內，更加難以偵測並下架

資安廠商 Guardio 旗下的資安專家，近期發現有駭侵者使用一種全新的手法來散布惡意程式碼；即利用區塊鏈來藏匿惡意程式碼，藉其去中心化的特性，使其駭侵手法更不容易偵測防範。

Guardio 在兩個多月前發現有駭侵者利用這種稱為「ClearFake」的手法來進行攻擊。原本該駭侵者係使用遭到入侵成功的 WordPress 網站來放置惡意程式碼，並利用 CloudFlare 的 Worker 功能進行重新導向；但因該 ClouldFlare Worker 遭發現而下架，之後駭侵者便改用 Binance Smart Chain 區塊鏈來存放其惡意程式碼。

Guardio 指出，駭侵者首先利用已知漏洞駭入多個 WordPress 網站，或是竊得該網站的 admin 登入權限，然後在其網站頁面中植入兩段指令碼，該指令碼會自 Binance Smart Chain 中載入惡意程式碼，再將這段惡意程式碼嵌入到 WordPress 的頁面中。這段程式碼會連線到一台控制伺服器，並載入第三段惡意軟體酬載；受害者如果不慎進入該受駭的 WordPress 網站，會看到假冒的 Chrome、Firefox、Edge 瀏覽器更新畫面，誘騙使用者按下更新按鈕並下載另一段惡意軟體。

Guardio 說，這種利用區塊鏈來放置惡意程式碼的手法十分新穎。由於區塊鏈具備去中心化與不可篡改的特性，因此置入到區塊鏈中的惡意軟體程式

碼是無法下架的。而 ClearFake 也利用區塊鏈來記錄控制伺服器的位置資訊，因此要是有某台控制伺服器遭到破獲下線，駭侵者也可在區塊鏈上輕鬆新增新伺服器的位址資訊。

這種利用區塊鏈來存放惡意程式碼的新手法，目前難以防治；以此案為例，僅能由加強 WordPress 網站本身的資安防護功能來入手。

- 資料來源：
  1. “EtherHiding” — Hiding Web2 Malicious Code in Web3 Smart Contracts
  2. Hackers use Binance Smart Chain contracts to store malicious scripts

2.2.2、詐騙集團利用以巴戰爭人道救援騙取加密貨幣捐款

近日在以巴戰爭造成眾多死傷與破壞時，資安專業媒體 BleepingComputer 的資安專家，發現有多組詐騙者利用各種社群管道發起詐騙募捐，誑騙網友以加密貨幣轉帳並侵吞愛心捐款。

BleepingCoumpter 報導指出，該社的資安專家發現在 X（舊名 Twitter）、Telegram 與 Instagram 上出現許多疑似詐騙募捐活動；駭侵者假冒各種公益慈善團體，要求網友以加密貨幣進行捐款轉帳，以做為戰爭受害者的人道救援之用；但其中有許多錢包位址都並非所宣稱的公益團體所擁有，明顯屬於詐騙。

其中一個假冒為「Gaza Relief Aid」（加薩救援協助）的所謂公益團體，在 Telegram 和 Instagram 上都開設了捐款帳號，並且列出其捐款錢包位址；但其使用的網域名稱「aidgaza[.]xyz」是在 2023 年 10 月 15 日才註冊完成，且不屬於任何已知的正牌公益團體所擁有。該網站的版型和內容直接盜用自真正的 Islamic Relief 救援團體官網，而其「最新消息」中的內容也盜自其他新聞網站，網站中放置了許多來自新聞媒體的戰地照片，且網站中也沒有附上該組織的地址、聯絡資訊等訊息。

據 BleepingComputer 追蹤其接受捐款的三個錢包位址，目前都沒有任何轉帳記錄。

另外，也有詐騙分子假冒為以色列方的人道救援組織，以類似手法企圖騙取愛心捐款；所幸到目前為止均無任何人捐款。

資安廠商 Kaspersky 也指出，該公司的資安研究人員截獲 500 封以上的詐騙電子郵件，同樣以搧動性的文字和圖片，企圖騙取收信人的愛心捐款；且有多個詐騙活動都使用同樣的錢包位址，顯見是同一詐騙集團所為。

建議在網路上進行愛心捐款時，捐款人務必多方查證，確認募款者為真，且募款方提供可查證的資訊，捐款才不致落入詐騙分子手中。

- 資料來源：
  1. Hackers exploit Israeli-Hamas war via fake donation emails, web links
  2. Palestine crypto donation scams emerge amid Israel-Hamas war

2.3、國際政府組織資安資訊

2.3.1、美國資安主管機關揭露前 10 大資安錯誤設定

美國國家安全局（National Security Agency, NSA）與網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）日前聯合發表資安指引，列出前 10 大最常出現的資安設定錯誤；建議各公私單位參考該指引，強化自身資安防護能力。

NSA 和 CISA 的這份指引，係由兩個單位內的資安紅隊與藍隊，針對各大公私單位組織的資安防護設定進行模擬攻防後所擬定，詳細說明各種駭侵者如何利用這些錯誤設定，以發動資安攻擊的策略、技術與程序（TTP），進行各種目的的攻擊，包括取得存取或控制權、資料或資源的竊取，以及如何鎖定機敏資訊或系統等等。

NSA 指出，接受其評估的美國政府單位，包括美國國防部、聯邦政府各民事行政部門、各州政府、地區行政單位、海外行政組織，以及多個私部門單位。

報告列出的 10 大資安錯誤設定如下：

- 使用軟體或應用程式的預設設定值；
- 未妥善區分一般使用者與管理者帳號權限；
- 內部網路監控不足；
- 網路分區設定不當；

- 軟體更新管理不當；
- 忽略系統存取控制限制；
- 多階段登入驗證防護薄弱或設定錯誤；
- 針對網路分享或服務的存取控制清單設定不夠妥善；
- 未能妥善進行密碼清理作業；
- 未限制程式碼執行。

CISA 官員也指出，上面列出的設定錯誤廣泛發生在多個大型單位，成為嚴重的資安防護漏洞，且軟體開發廠商未能在設計時以資安防護為優先考慮，使得使用單位還需費力進行額外防護。

建議可以依 NSA 與 CISA 要求檢視單位的資安防護是否存有上述問題，並且立即採取對策加以彌補，包括停止使用預設帳號密碼與安全設定值、停用未經使用的網路服務、強化資源存取權限控管、經常更新系統，且在第一時間更新已發布的漏洞。

- 資料來源：
  1. NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations
  2. NSA and CISA reveal top 10 cybersecurity misconfigurations

2.3.2、美國資安主管機關公布勒贖團體經常攻擊的漏洞與錯誤設定

美國資安主管機關「網路安全暨基礎設施安全局」（Cybersecurity and Infrastructure Security Agency, CISA），日前公布一批勒贖攻擊團體經常用於攻擊的漏洞與資安設定錯誤樣態，目的是要協助關鍵基礎設施強化資安防護能力。

CISA 於 2023 年 1 月起開始推動「勒贖軟體漏洞警告先導計畫」（Ransomware Vulnerability Warning Pilot, RVWP）專案，並且經常新增相關資訊；本次公布的資訊即屬 RVWP 專案的防護資訊更新。

至今為止，CISA 的 RVWP 計畫已經公布超過 800 個經常遭到勒贖團體攻擊使用的各式軟體與系統的資安漏洞與錯誤資安設定，其目的在於提供各種經常遭勒贖攻擊鎖定的全球關鍵基礎設施或服務，依其指引提升資安防護量能，避免因為遭到勒贖攻擊而導致關鍵基礎設施服務中斷，因而造成重大影響。

CISA 指出，雖然該單位過去已經推出「遭攻擊已知漏洞」（Known exploited vulnerabilities, KEV）清單供各公私單位參考使用，且在該清單中額外加上一個欄位，專門標示易遭勒贖攻擊駭侵者使用的資安漏洞，但為因應日益猖獗的勒贖攻擊，CISA 決定推出 RWVP 通報，以強化針對勒贖攻擊的防護量能。

CISA 也同時推出一個專為防杜勒贖攻擊的入口網站「StopRansomware.gov」，其目的在於集中提供各種防範並處理勒贖攻擊的

多種有用資訊。

建議各公私單位可參考 CISA 提供的各類資安防護通報，並依其指引提升防護能力，以提高安全性。

- 資料來源：
  1. GUIDANCE AND RESOURCES
  2. Ransomware Vulnerability Warning Pilot updates: Now a One-stop Resource for Known Exploited Vulnerabilities and Misconfigurations Linked to Ransomware
  3. CISA shares vulnerabilities, misconfigs used by ransomware gangs

2.3.3、奧地利警方破獲網路電視影片盜播網

奧地利警方日前宣布破獲一個大型國際版權影片盜播 IPTV 網路，該執法行動同步於維也納、下奧地利、薩爾茲堡等多個城市展開，除了逮捕 20 人之外，也破獲多台網路電腦設備與該集團的不法獲利達 160 萬歐元。

奧地利警方指出，該集團自 2016 年開始販售經過破解的加密版權電視節目觀看服務；奧國警方是在接獲德國方面的報案後開始進行調查，終於破獲這個共有 80 名嫌犯的大型盜版犯罪集團，嫌犯全數為土耳其國籍。

警方指出，該盜版集團成員中有負責破解加密電視訊號的內容提供者，也有負責招募訂戶的經銷商；經銷商以一年 50 美元的價格購買盜播網會員資格後，再以一年 200 美元的價格販售給想看盜版電視節目的網友。

警方說，每名經銷商手上約有 300 到 2,500 名訂戶，經銷商雖然會使用 Facebook 廣告進行宣傳，但主要的客戶來源以口耳相傳為主。

警方破獲的設備，包括 35 台用於訊號解碼與 IPTV 廣播的伺服器，以及 55 台電腦、硬碟、智慧型手機等，甚至還包括一台 Audi A7 豪華轎車。

警方說，主要的嫌犯靠盜版生意賺取大筆不法收入，除了擁有多輛豪華轎跑車外，也擁有多筆豪宅、多家公司、俱樂部等。

警方表示遭到逮捕的嫌犯，包括 3 名內容提供者與 15 名經銷商，都將以商業詐騙、洗錢、著作權侵權等罪名遭到起訴，尚未落網的嫌犯主要都在德國境內，目前也已掌握其犯罪地點的相關情報。

建議使用網路影音的觀眾，不應安裝來路不明的盜版影音機上盒或加入盜版網站會員，以免同時吃上侵害著作權的官司，面臨鉅額罰款。

- 資料來源：
  1. Hotel hackers redirect guests to fake Booking.com to steal cards

2.3.4、印度發動全國執法行動，查緝網路與加密貨幣詐騙分子

印度中央調查局（Central Bureau of Investigation, CBI）日前指揮多個印度執法單位，同步於全印度 76 個地點展開全國網路犯罪大型查緝活動，以扼止各種網路詐騙活動。

這波大規模查緝的行動代號為 Operation Chakra-II，主要目標是要阻斷各種透過網路進行的金融犯罪集團運作。CBI 會同多個國際、國內執法單位和 Microsoft、Amazon 等跨國科技巨頭，共同展開這次執法行動。

這次展開掃蕩活動的地點多達 76 處，分別位於印度 Tamil Nadu、Pubjab、Bihar、Delhi、West Bengal 等省分；執法人員一共緝獲 32 部行動電話、48 部筆記型電腦與硬碟，以及 33 張 SIM 卡。

據 CBI 指出，這次執行行動也破獲 2 個涉嫌假冒 Microsoft 和 Amazon 客服支援中心的攻擊活動。該攻擊活動已進行長達 5 年以上，受害者多達 2,000 人以上，且分布遍及美國、加拿大、德國、澳洲、西班牙、英國等。

這批駭侵者會利用惡意軟體，在訪客電腦中顯示詐騙支援訊息，謊稱客戶的系統發生問題，需要撥打免費客服專線電話。當受害者撥打該電話後，由駭侵者假冒的客服人員，就會謊稱客戶的電腦系統發生嚴重問題，藉以收取高額維護費用。

根據美國聯邦調查局在 2022 年的網路犯罪調查報告指出，假冒客服人員的詐騙案件，在 2018 年到 2022 年間高居各式網路犯罪的前五大類型之一。

單在 2022 年一年之間，這類詐騙造成的財務損失就高達 8 億美元。

建議各公私單位應隨時加強資安防護，如遇疑似詐騙客服，要求高額維修費用，應立即洽詢原廠管道進行確認。

- 資料來源：
  1. India targets Microsoft, Amazon tech support scammers in nationwide crackdown

2.4、社群媒體資安近況

2.4.1、惡意軟體 DarkGate 透過遭駭 Skype 與 Teams 帳號散布

資安廠商趨勢科技 (Trend Micro) 日前發表研究報告，指出該公司發現一個名為 DarkGate 的惡意軟體，近期利用竊得的 Skype 帳號，以訊息傳遞含有惡意軟體指令檔的附件給目標攻擊對象來發動駭侵攻擊。

趨勢科技的研究人員，在 2023 年 7 月到 9 月間觀察到 DarkGate 的一波攻擊行動；駭侵者利用不明方式駭入某些 Skype 帳號並混入該帳號進行中的對話，然後將含有惡意軟體的檔案名稱，改成符合對話內容的形式後傳遞給受害者。

傳送給受害者的檔案中，含有 VBA 載入指令，可進一步載入 AutoIT 惡意軟體酬載，用來載入並執行最終的 DarkGate 惡意軟體酬載。

趨勢科技指出，目前並不清楚這些 Skype 帳號是如何遭到竊取，以用於發送惡意軟體的，有可能是來自於駭侵討論區或暗網中出售的使用者登入資訊。

此外，趨勢科技也觀察到 DarkGate 駭侵者試圖透過駭入企業通訊用的 Microsoft Teams 對話串來散布 DarkGate 惡意軟體與其他釣魚惡意程式碼；遭到攻擊的主要是開放給企業外部使用者加入對話的 Teams 工作群組對話。

趨勢科技指出，駭侵者係利用已遭到攻擊竊取的企業外部 Office 365 使用者帳號，並使用可輕易取得的駭侵工具 TeamsPhisher 來發動攻擊；駭侵者

利用該工具來跳過針對 Microsoft Teams 外部使用者的檔案分享限制，並且發送釣魚附件檔案給討論群組中的使用者。

建議企業加強對內部訊息討論群組的資安防護，分享相關文件、試算表或簡報應盡可能避免直接分享檔案，可改使用線上版生產力工具，以杜絕惡意指令碼的執行。

- 資料來源：
  1. DarkGate Opens Organizations for Attack via Skype, Teams
  2. DarkGate malware spreads through compromised Skype accounts

2.4.2、駭侵團體假冒 Cosair 在 LinkedIn 上徵才，藉機散布惡意軟體

資安廠商唯思安全（WithSecure）近期發現有駭侵者假冒電腦硬體製造商 Cosair 在 LinkedIn 上刊登徵才啟事，藉以散布 DarkGate 和 RedLine 等惡意軟體。

WithSecure 的資安專家在該公司發表的資安研究報告中指出，近來有駭侵者在 LinkedIn 上冒充專業電腦硬體製造商 Cosair 發布一個負責投放 Facebook 廣告的假職缺，當有受害者上鉤後，駭侵者再傳送一個含有惡意軟體文件的 zip 壓縮檔給受害者，以在受害者電腦中散布惡意軟體。

WithSecure 指出，發動這波攻擊的駭侵團體，也曾在去年發動另一波名為「Ducktail」駭侵攻擊活動。

這波攻擊的主要目的，是要竊取受害者管理的 Facebook 企業帳號，藉以進行進一步的駭侵攻擊活動，或是將帳號出售牟利。主要的攻擊對象為美國、英國和印度的求職者；而假冒的 LinkedIn 求才啟事主要招募的是具有 Facebook 企業帳號與 Facebook 廣告投放經驗的社群管理者。

受害者一旦下載了含有惡意軟體的 zip 檔，解壓縮後會出現三個檔案，其中一個 .docx 檔案中含有惡意 VBS 指令碼；開啟該 Word .docx 檔案時，會進一步下載 DarkGate 或 RedLine 惡意軟體酬載，並且試圖移除受害系統上的資安防護軟體，以隱蔽行蹤並持續進行攻擊。

建議使用者在 LinkedIn 等類似的社群網站上，應對任何附件檔案提高警

覺，勿輕易開啟容易夾藏惡意程式碼的檔案格式，如 Microsoft Office 文件檔與各種可執行檔。

- 資料來源：
  1. DarkGate attacks linked to Vietnam-based cyber criminals
  2. Fake Corsair job offers on LinkedIn push DarkGate malware

2.5、行動裝置資安訊息

2.5.1、Android 10 月更新包修復 54 個漏洞，部分已遭用於駭侵攻擊

Google 近期推出 2023 年 10 月份 Android 軟體更新，適用於 Android 11 到 Android 13，一共修復多達 54 個資安漏洞，其中已有 2 個漏洞已遭駭侵者用於攻擊活動。

遭到駭侵者用於攻擊的資安漏洞，分別是 CVE-2023-4863 與 CVE-2023-4211；Google 在資安通報中指出這兩個漏洞已用於有限度的目標針對攻擊之中。

CVE-2023-4863 是一種存於泛用型開源程式庫 libwebp 的緩衝區溢位（buffer overflow）錯誤，許多大型知名軟體如 Chrome、Firefox、iOS、Microsoft Teams 等都受此漏洞衝擊而成為駭侵者的攻擊目標。

由於這個漏洞的影響範圍甚廣，不同受影響的公司都分別提出了漏洞通報；後來都歸納在 CVE-2023-4863 這個 CVE 編號之下。

而 CVE-2023-4211 是個存於 ARM 處理器中 Mali GPU 驅動程式的記憶體釋放後使用（use-after-free）漏洞，駭侵者可藉以在本地端存取或操弄機敏資料。

總體來說，這次的 Android 2023 年 10 月份資安更新，解決的漏洞存在的部分分列如下：

- Android Framework：13 個；
- 系統組件：12 個；
- Google Play：2 個；
- ARM 組件：5 個；
- Unisoc 晶片相關：1 個；
- Qualcomm 晶片相關：18 個（其中有 15 個為閉源）

而在漏洞的危險程度方面，這 54 個獲得修復的漏洞中，有 5 個列為「嚴重」(critical）等級，另有 2 個屬於遠端執行任意程式碼漏洞。Google 將分成兩波推出更新，第一波於 10 月 1 日推出，主要修復 Android 核心組件的漏洞，第二波則在 10 月 6 日推出，主要處理系統核心和閉源組件的漏洞。

由於多數的 Android 裝置都無法直接套用 Google 推出的系統更新，必須等待裝置製造商推出更新，因此用戶應密切注意更新的推出，且在等待期間應避免各種危險操作行為，例如自不明來源下載 apk 檔案等。

- 資料來源：

1. Android 安全性公告 - 2023 年 10 月
2. Android October security update fixes zero-days exploited in attacks

2.5.2、Gooogle Play Store 推出惡意軟體即時掃瞄功能

Google 日前宣布在其 Android 應用程式商店 Google Play Store 的 Google Play Protect 保護機制中推出全新惡意軟體即時掃瞄功能，以強化該平台對於 Android 平台上日益猖獗惡意軟體的防護能力。

Google Play Protect 是 Google Play Store 中內建的主要防護機制，可在裝置上進行惡意軟體掃瞄，每日總掃瞄次數可達 1,250 億次。該工具不只可掃瞄下載自 Google Play Store 的應用軟體，也可以掃瞄自第三方 App Store 或網路上不明來源處下載的 APK 檔案。

過往駭侵者常會利用「安裝後載入」的手法來規避 App 上架到 Google Play Store 時的惡意軟體掃瞄措施，方法是在上架 Google Play Store 時先上架無害的版本，待使用者下載安裝到其裝置後，再從外部伺服器載入惡意軟體酬載。

為防止駭侵者繼續以這種方式植入惡意軟體，強化版的 Google Play Protect 會在裝置上進行掃瞄，並將掃瞄結果傳送到 Google Play Protect 的後端架構進行程式碼分析，同時以機器學習來累積掃瞄經驗；，一旦發現惡意軟體訊號時，即會通知使用者。

Google 目前已在印度和部分指定國家推出 Google Play Protect 新機制，且會陸續在全球其他國家推出。

資安專家指出，Google 這套新系統雖然無法防杜所有 Android 平台上的

惡意軟體，但應能有效降低該平台上過去未能偵測出的惡意軟體數量。

專家也表示，惡意軟體開發者當然也會試圖找出這套系統的弱點，因此加強使用者自我保護的觀念與使用習慣，仍然十分重要。

建議 Android 平台使用者在此系統可使用時下載安裝，且仍應維持良好習慣，絕不安裝來路不明的 APK 檔案。

- 資料來源：
  1. Google Play Protect adds real-time scanning to fight Android malware
  2. Use Google Play Protect to help keep your apps safe and your data private

2.5.3、資安專家發現 Android 木馬惡意軟體，可盜錄通話內容

資安廠商 F-Secure 近日發現一個名為 SpyNote 的 Android 木馬軟體捲土重來，再度展開大規模攻擊，竊取使用者通訊內容中的金融資訊，以竊取受害者帳戶中的資金。

這個名為 SpyNote 的 Android 木馬惡意軟體，首次發現是在 2022 年；據資安廠商的報告指出，這次 SpyNote 仍透過「Smishing」方式感染，即透過惡意釣魚簡訊發送含有惡意軟體 apk 檔下載連結的簡訊給潛在受害在，使用者如果點按該連結，並在自己的 Android 手機上安裝該 apk 檔案，就會遭到該惡意軟體的感染。

接下來 SpyNote 會要求使用者給予各種權限，甚至會自己產生點按動作，代替使用者授予全部系統服務存取權限，接著就會在使用者的 Android 手機中建立背景服務，開始將使用者手機中的各項資訊，包括盜錄用戶的通話內容錄音、擅自進行畫面截圖或錄影、記錄使用者的輸入按鍵與通聯對象記錄、各種服務的登入資訊、手機所在地的地理座標資訊等等，並將這些資訊傳送到駭侵者設立的控制伺服器。

此外，如同多種 Android 惡意軟體，SpyNote 也有多種設計以防遭使用者移除；除了隱藏該 App 的 icon，讓使用者難以發現之外，也會利用 Android 的內部系統服務來混淆其存在，使得 SpyNote 極難移除；如想完全移除，使用者只能將 Android 手機重置為出廠狀態。

Android 使用者應避免自來路不明處下載安裝任何 apk 檔案，例如即時通

訊、網路討論區、不明人士傳來的簡訊等，以避免遭惡意軟體潛入裝置。

- 資料來源：
  1. Take a note of SpyNote!
  2. Android trojan spotted in the wild can record audio and phone calls

2.5.4、多個 Android 惡意軟體上架 Google Play Store，下載達 200 萬次

資安廠商 Doctor Web 旗下的資安研究人員，近來發現有多個惡意 Android 應用軟體成功上架到官方應用程式商店 Google Play Store 內，假扮成各種遊戲來誤導使用者下載安裝；其總下載安裝次數突破 200 萬次。

研究人員指出，這些 App 內含的多半是 FakeApp、Joker、HiddenAds 的惡意軟體，其中 FakeApp 會將使用者導向投資詐騙網站或是網路賭場、Joker 會擅自訂閱高價服務，騙取訂閱費用分潤，而 HiddenAds 則是廣告惡意軟體，會不斷在使用者手機上顯示大量廣告。

據 Doctor Web 的報告指出，含有 FakeWeb 的惡意 Android 應用軟體，下載次數最多的如下：Eternal Maze (50,000 次)、Jungle Jewels (10,000 次)、Stellar Secrets (10,000 次)、Fire Fruits (10,000 次)、Cowboy′ s Frontier (10,000 次)、Enchanted Elixir (10,000 次)。

內含 Joker 的惡意 Android App，下載次數較多的則有：Love Emoji Messenger (50,000 次)、Beauty WallPaper HD (1,000 次)。

內含 HiddenAds 惡意軟體的 Android App 下載次數則遠多於上述二者，包括 Super Skibydi Killer (1,000,000 次)、Agent Shooter (500,000 次)、Rainbow Stretch (50,000 次)、Rubber Punch 3D (500,000 次)。

建議 Android 使用者即使在官方 Google Play Store 中下載安裝軟體前，都應提高警覺，仔細閱讀其他使用者評價，再決定是否下載安裝。

- 資料來源：
  1. Doctor Web’s September 2023 review of virus activity on mobile devices
  2. Android adware apps on Google Play amass two million installs

2.6、軟體系統資安議題

2.6.1、Microsoft 緊急推出 Edge、Teams 更新，修復 2 個開源組件中的 0-day 漏洞

Microsoft 日前緊急針對旗下的 Microsoft Edge、Teams 與 Skype 緊急推出軟體更新，修復 2 個存於開源程式庫中的 0-day 漏洞。

第一個獲得修復的漏洞是 CVE-2023-4863，這個漏洞存於開源 WebP 程式庫 libwebp 中，屬於 heap 緩衝區溢位（buffer overflow）錯誤；駭侵者可透過此漏洞造成應用軟體崩潰，亦可執行任意程式碼。

值得注意的是，由於 libwebp 這個開源程式庫是用來對 WebP 格式的網路圖片進行編碼與解碼，因此應用範圍十分廣泛；除了 Microsoft 這次修復的三個產品外，包括 Safari、Mozilla Firefox、Opera、Android 原生瀏覽器之外，像是 1Password 與 Signal 等熱門應用軟體也採用了 libwebp，因此都需進行資安修補。

第二個獲得修復的漏洞是 CVE-2023-5217，這個漏洞存於開源 VP8 程式庫 libvpx 中的視訊編碼程式，和前一個漏洞一樣屬於 heap 緩衝區溢位（buffer overflow）錯誤；駭侵者也可透過此漏洞造成應用軟體崩潰，亦可執行任意程式碼。

而 libvpx 這個開源程式庫，因為負責處理 VP8 和 VP9 兩種影片格式的編解碼，因此 同樣廣泛應用在多種軟體之中，包括多種影音串流平台的 App 如 Netflix、YouTube、Amazon Prime Video 等也都使用。

目前已知有駭侵者利用這兩個影響廣泛的漏洞，來發動間諜軟體攻擊，使用者應特別提高警覺。

建議使用 Microsoft 以上產品的使用者，應儘速套用更新，以免遭到駭侵者透過已知漏洞發動攻擊。

- 資料來源：
  1. Microsoft’s Response to Open-Source Vulnerabilities - CVE-2023-4863 and CVE-2023-5217
  2. Microsoft Edge, Teams get fixes for zero-days in open-source libraries

2.7、軟硬體漏洞資訊

2.7.1、多款路由器遭植入 Mirai DDoS 僵屍網路變種惡意軟體

Fortinet 旗下的資安專家，近期發現一個稱為 IZ1H9 的 Mirai DDoS 僵屍網路，最近新增了多達 13 種變種，以各廠牌型號基於 Linux 作業系統的路由器產品為目標加以攻擊。

Fortinet 的資安專家發現在 2023 年 9 月的第一周，由 IZ1H9 發動的攻擊次數達到近期的高峰，偵測到針對弱點裝置多達數萬次的攻擊行動。

IZ1H9 的典型攻擊手法是利用各廠牌網通產品的漏洞加以攻擊，植入 Mirai 變種 DDoS 僵屍網路程式，使該裝置成為其攻擊網路的一部分，再針對「租用」其服務的客戶需求，攻擊特定的網路目標。

這次 Fortinet 發現的新變種，分別鎖定攻擊的路由器廠牌與版本，包括 D-Link 多款產品、Netis WF2419、Sunhillo SureLine 8.7.0.1.1 之前版本、Geutebruck 多款產品、Yealink Device Management 3.6.0.20、Zyxel EMG 3525/VGM1312 V5.50 之前版本、TP-Link Archer AX21 (AX1800)、Korenix Jetware wireless AP、TOTOLINK 多款路由器產品等；主要都是透過這些產品已知但未及時更新的漏洞。

1Z1H9 在感染上述廠牌型號的路由器產品後，會先自一個特定 URL 載入名為 l.sh 的指令檔，執行該指令檔後，先行刪除路由器內的 log 檔案，以隱匿入侵行為，然後根據產品型號的不同，下載不同的酬載惡意軟體檔案，之後

會修改路由器的 iptables 規則，並且將其連線轉到特定連接埠，以藏匿其連線動作，減少被阻擋的機會。之後該惡意軟體就會連線到其控制伺服器，等待攻擊命令下達後，再發動包括 UDP、UDP Plain、HTTP 泛濫、TCP SYN 等類型的 DDoS 攻擊。

- 解決方案：建議各受影響廠牌路由器之用戶應立即更新到最新版本韌體，未提供更新者應考慮替換為較新機種。

- 資料來源：
  1. IZ1H9 Campaign Enhances Its Arsenal with Scores of Exploits
  2. Mirai DDoS malware variant expands targets with 13 router exploits

2.7.2、Google 修復已遭用於攻擊的 Chrome 0-day 漏洞

Google 日前推出 Google Chrome 瀏覽器的新版本 117.0.5938.132，修復一個已證實遭到駭侵者用於攻擊的 0-day 漏洞 CVE-2023-5217；Google Chrome 與各相容 Chromium 的瀏覽器使用者應盡速更新至最新版本。

這個 CVE-2023-5217 的漏洞，存於 Google Chrome 瀏覽器內建的開源 libvpx 視訊解碼程式庫中的 VP8 編碼單元，屬於 heap 暫存器溢位錯誤；駭侵者將可利用此漏洞來造成 App 執行崩潰，亦能藉以執行任意程式碼。

CVE-2023-5217 這個漏洞的 CVSS 危險程度評分高達 8.8 分（滿分為 10 分），危險程度評級為「高｜（high）。

Google 也在日前發表的資安通報中指出，該公司已獲悉 CVE-2023-5127 已遭駭侵者用於攻擊的情資；Google 表示，在大多數使用者都已經更新到新版 Google Chrome 瀏覽器，且第三方程式庫已經更新該漏洞之前，Google 不會公布任何關於此漏洞的細節資訊。

Google 也自即日起逐步釋出新版 Google Chrome 瀏覽器以修復此漏洞；新版本的編號為 117.0.5938.132，使用者可望在近日在 Google Chrome 瀏覽器中收到更新通知；但其他以開源的 Chromium 製作的 Chrome 相容瀏覽器，可能要稍後才能陸續更新。

- CVE 編號：CVE-2023-5217

- 影響產品(版本)：Google Chrome 版本 117.0.5938.132 之前版本，包括 Windows、Mac、Linux 等
- 解決方案：更新至 Google Chrome 117.0.5938.132 與後續版本。

- 資料來源：
  1. Stable Channel Update for Desktop
  2. CVE-2023-5217
  3. CVE-2023-5217 Detail

2.7.3、Microsoft 推出 2023 年 10 月 Patch Tuesday 每月例行更新修補包，共修復 104 個資安漏洞，內含 3 個 0-day 漏洞

Microsoft 日前推出 2023 年 10 月例行資安更新修補包「Patch Tuesday」，共修復 104 個資安漏洞；其中含有 3 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 104 個，較上個月（2023 年 9 月）的 59 個資安漏洞大為增加；而在這 104 個漏洞中，僅有 12 個屬於「嚴重」等級，另有 3 個是屬於已知遭到駭侵者用於攻擊的 0-day 漏洞，另外還有 45 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。

- 執行權限提升漏洞：26 個；
- 資安防護功能略過漏洞：3 個；
- 遠端執行任意程式碼漏洞：45 個；
- 資訊洩露漏洞：12 個；
- 服務阻斷（Denial of Service）漏洞：17 個；
- 假冒詐騙漏洞：1 個；
- Edge -Chromium 漏洞：1 個。

本月的 Patch Tuesday 有 3 個已遭大規模濫用的 0-day 漏洞，其中兩個如

下：

第一個 0-day 漏洞是 CVE 編號為 CVE-2023-41763，存於 Skype for Business 中，屬於執行權限提升漏洞；駭侵者可透過此漏洞，提高自身的執行權限，並且檢視某些機敏資訊；不過微軟也指出該駭侵者僅能利用此漏洞存取部分資訊，且無法竄改資訊內容。

第二個值得注意的 0-day 漏洞是 CVE-2023-36563，是存於 Microsof WordPad 中的資訊洩露漏洞，駭侵者可利用此漏洞，在開啟 WordPad 文件時竊取 NTLM 雜湊資料 ，並用以進行 NTLM 中繼攻擊。

- CVE 編號：CVE-2023-41763、CVE-2023-36563 等
- 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 用戶應立即依照指示，以最快速度套用 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. Skype for Business Elevation of Privilege Vulnerability
  2. Microsoft WordPad Information Disclosure Vulnerability
  3. Microsoft October 2023 Patch Tuesday fixes 3 zero-days, 104 flaws

第 3 章、 資安研討會及活動

TWCERT 2023 台灣資安通報應變年會	
活動時間	**112 年 11 月 14 日(星期二)上午 09 時 00 分至 16 時 00 分**
活動地點	**本活動為線上直播觀看，敬請點選下方連結或掃描 QRcode 填寫報名資料，經審核後將透過電子郵件寄送活動直播連結，敬請踴報名。**
活動網站	**https://twcert.informationsecurity2023.com.tw/** **https://twcert2023conference.kktix.cc/events/11142**
活動概要	 **主辦單位： TWNIC、TWCERT/CC** 活動主題：韌性資安 永續台灣 數位時代下，資訊安全的韌性和永續性至關重要。企業通過強化資安策略、技術及人才，落實公私資安聯防，以應對不斷擴大與翻新的網路攻擊，確保數位永續，同時強化全球跨領域合作，才能實現數位韌性與永續營運。 如有任何問題，敬請以 email 聯繫：davidhuang@greatasia168.com.tw

第 40 屆 TWNIC IP 政策資源管理會議	
活動時間	**2023 年 11 月 16 日(四) 9:00-16:30**
活動地點	**臺大醫院國際會議中心 402AB，並提供 YouTube 線上觀看**
活動網站	**https://opm.twnic.tw/40th/index.html**
活動概要	 **主辦單位： TWNIC** 為提供臺灣網路界一個可以討論 IP 網路技術相關議題的社群與機制平台，TWNIC 將於 11 月 16 日舉辦「第 40 屆 TWNIC IP 政策資源管理會議」。 場場精彩可期，誠摯邀請您能一同參與！ 本次會議專題演講邀請 APNIC 首席科學家 Geoff Huston 及中華電信何業勤協理，介紹 On LEOs (Low Earth Orbuts) and Starlink 低軌衛星和星鏈及台灣衛星網路服務的發展。此外，網際安全特別興趣小組 (Cyber Security SIG) 場次，特別邀請國家資通安全研究院及中華資安國際專家講者，介紹資安政策和技術的發展，其他場次包含維運技術、國際合作、網路政策管理及 IPv6 佈建發展分享等主題。也安排傳輸層協定 QUIC 重要性和發展的介紹，希望讓各界進行網路技術研究、產業發展之溝通交流，促進網際網路相關產業發展。 歡迎大家踴躍報名參加!

【資安學院】11/23 網軍攻擊手法實務課程-DDoS 原理與實務	
活動時間	**2023-11-23 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/3970**
活動概要	 **主辦單位： 中華民國資訊軟體協會** 費用： 原價：NT 3,300 元/人 早鳥價： NT 3,000 元/人(開課前一個月需完成報名及繳費) 軟協會員：NT 2,800 元/人 費用含稅、教材及完課證明 網路攻擊幾乎無所不在，國際網軍時時刻刻對企業、政府機構、學校機關、甚至關鍵基礎設施等等發動攻擊，除了竊取機密資料、換置網頁，也不斷地建立擴增殭屍網路的規模與覆蓋範圍。分散式拒絕服務(DDoS) 攻擊，攻擊者會使用多個盜用或受控的來源來產生攻擊。 課程主要是在於教導、介紹一些駭客 DDoS 原理與實務常用的工具和方法，藉以實際了解 DDoS 攻擊手法，進而知道如何保護快攻與慢打攻擊手法分析及防禦。透過互動與實務操作，教導您如何 DDoS 防禦手法介紹與實作的安全漏洞，藉以保護系統安全，課程中將加強實際的上機操作，針對系統安全讓您有更深一層的了解，藉由上課所模擬

	的網路環境中，了解駭客如何 DDoS 攻擊事件分析及防禦，您也將學到如何制定策略、權限，以防堵不法駭客的入侵。 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： 2023-11-20

第六屆物聯網安全高峰論壇	
活動時間	**2023/11/29 09:00-17:00**
活動地點	**華南銀行國際會議中心(台北市信義區松仁路 123 號)**
活動網站	**https://www.mem.com.tw/event/IoT_Security/index.html**
活動概要	 **主辦單位：新電子科技雜誌、新通訊元件雜誌、網管人雜誌** AI 應用遍地開花　物聯網安全風險加劇 打造安全可信 AIoT 創新應用 「物聯網安全高峰論壇」是前瞻物聯網資安趨勢指標性技術盛會 匯聚產官學研近 20 位權威專家，深度解析 AI 對 IoT 安全帶來的最新挑戰 同時分場討論 5G AIoT/工控/車用資安技術新知 讓您同時掌握產業宏觀視野與具體實戰攻略 以更強韌的「物聯網安全」，迎向「安全物聯網」大商機

【資安學院】11/29 網路封包與事件解析	
活動時間	**2023-11-29 09:30~16:30 / 報名截止：2023-11-24**
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	
活動概要	 **主辦單位：中華民國資訊軟體協會** 費用： 原價：NT 8,000 元/人 早鳥價： NT 7,200 元/人(開課前一個月需完成報名及繳費) 軟協會員：NT 6,800 元/人 費用含稅、教材及完課證明 網路封包與事件分析有著密不可分的關係，網管人員與資安事件調整人員經常透過網路封包找出環境中可能的存在的資安問題，本課程著重在介紹網路通訊中常用通訊協定原理介紹、分析與應用，包含上機實作，透過課程教學與實務操作，解說資安分析工具詳細操作與使用，使學員熟悉封包擷取、BFP 過濾器及常用操作技巧，研判網路封包等行為。 聯絡窗口： 02-2553-3988 分機 388、816　廖資深專員、林專員 security@cisanet.org.tw

第 4 章、 2023 年 10 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。

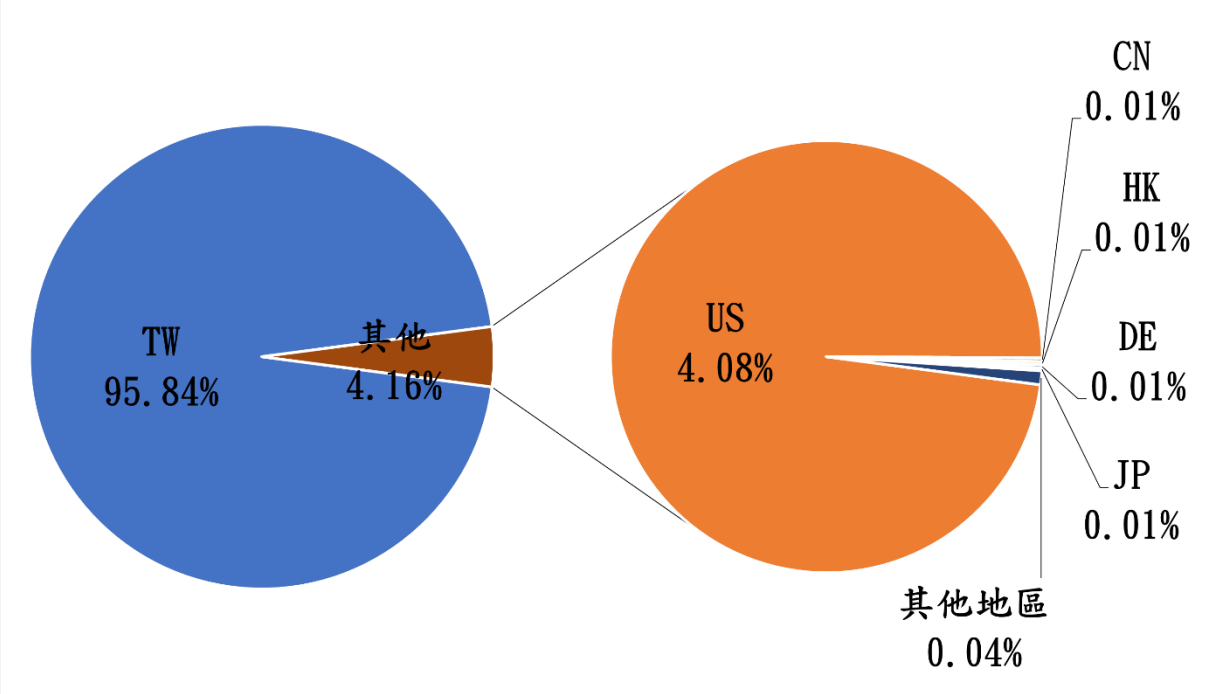

圖 1、分享地區統計圖

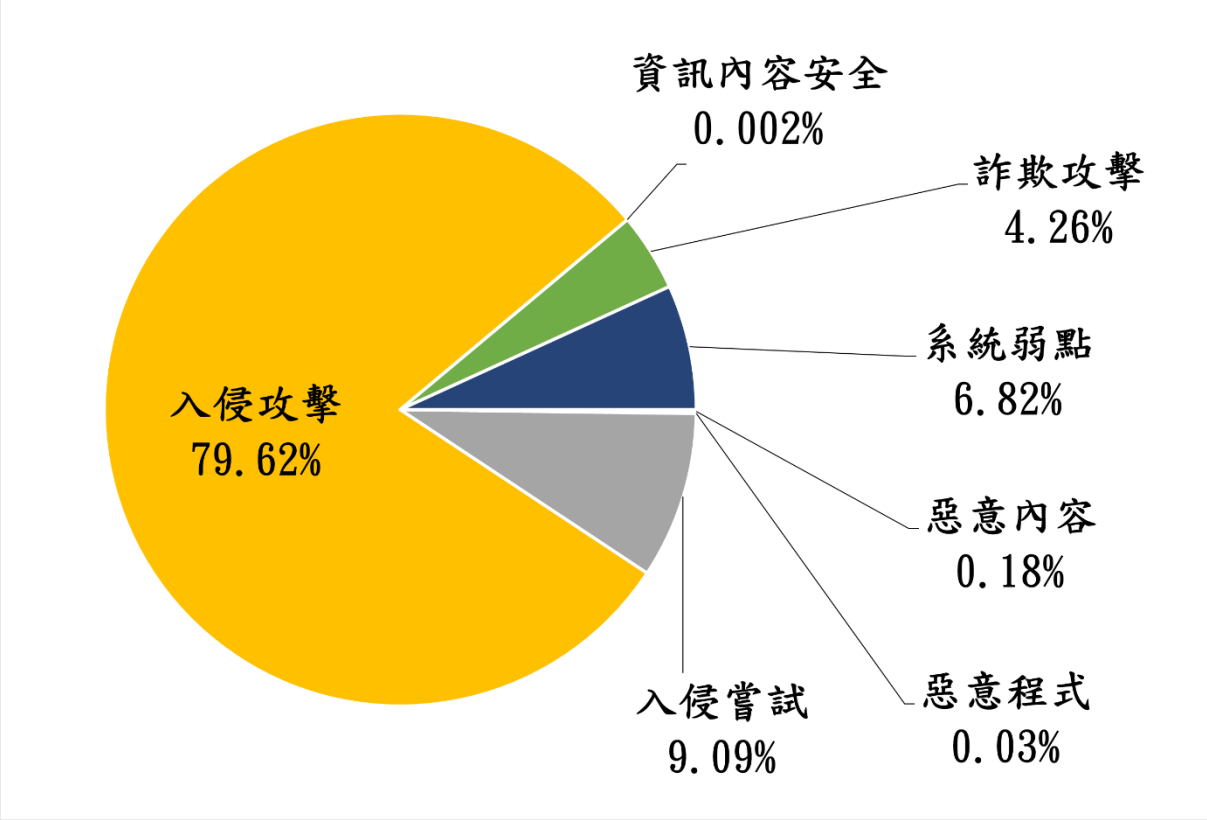
資訊內容安全
0.002%
詐欺攻擊
4.26%
系統弱點
6.82%
惡意內容
0.18%
惡意程式
0.03%
入侵嘗試
9.09%
入侵攻擊
79.62%

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 11 月 10 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**