TWCERT/CC 資安情資電子報

2023 年 8 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 6 章節：

第 1 章、封面故事：TWCERT/CC 2022 資安年刊。

第 2 章、資訊安全宣導：針對近期資安議題、TWCERT/CC 服務或配合政府資安政策等進行資安宣導，以提升大眾資安意識。

第 3 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 4 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。

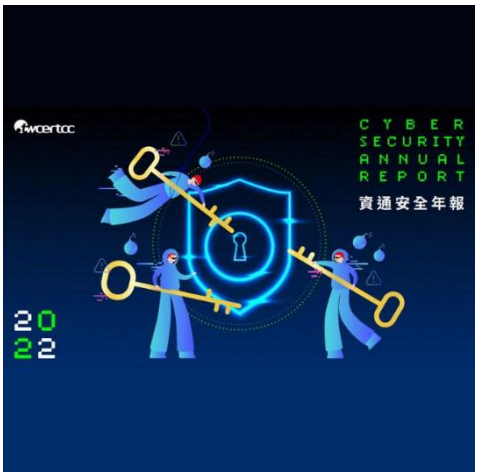
第 5 章、TVN 漏洞公告：TWCERT/CC 為 CVE 編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明上月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN)平台之漏洞嚴重程度前五的產品漏洞資訊。

第 6 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

TWCERT/CC 2022 資安年刊



想了解 2022 年 TWCERT/CC 都在做什麼嗎？

2022 大資安事件及資安通報狀況又如何？

那就讓我們一起透過年刊回顧一下！

- 請點此觀看 TWCERT/CC 2022 資安年刊

第 2 章、 資訊安全宣導

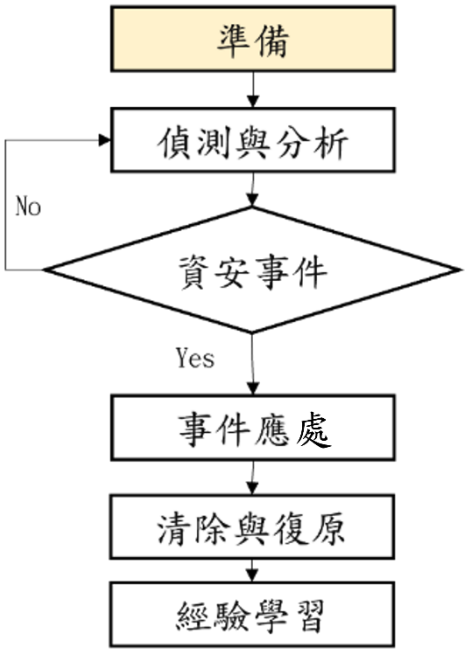
2.1.1、偽冒機關或組織之釣魚網站情資

本中心近期接獲通報，在搜尋引擎使用關鍵字 taxi-lyon-rs 或 site:*.fr，並加上特定公、私機關(行號)的名稱，會查詢到偽冒相關機關或組織的釣魚網站。

1. 提醒民眾，不點擊不明的網址或連結，進入可疑網站不輸入個資、帳號密碼及金融資訊，更不要進行匯款。
2. 政府機關網站的網址會以 https 開頭，以 gov.tw 結尾。
3. 建議各企業針對上述手法，對相關域名進行阻擋。
4. 若發現可疑網址或網站，可以至 TWCERT/CC 的 Phishing Check 網路釣魚通報進行通報，經確認後 TWCERT/CC 會協助釣魚網站下架服務。

2.1.2、企業資安事件應變處理指南之事前準備

事件處理的第一階段為「準備階段」，將針對資安事件處理之工具、文件、人員、管理制度進行規劃與準備。



1、資安工具準備

工欲善其事，必先利其器，建議準備資安工具以儲存媒體離線保存(例如：具備防寫開關的隨身碟或記憶卡)並定期更新，其中劃分為 5 個類別，分別為：1.網路檢測、2.檔案檢測、3.系統檢測、4.記憶體取證及 5.弱點掃描，參考工具列表如下：

項次	類型	工具名稱
1	網路檢測	Snort、Wireshark、Nmap、Angry IP Scanner、TCPView
2	檔案檢測	Msert、VirusCheck、PE Studio、VirusTotal
3	系統檢測	ProcessExplorer、Autoruns、eventvwr、Regedit
4	記憶體取證	FTK Imager、volatility
5	弱點掃描	Nessus、OpenVas

2、資安事件分類分級

為了掌握資安事件應變的時效性，依照資安事件影響的嚴重性劃分等級，並設定回報時限，依組織業務營運狀況建議分為四個等級。

一級資安事件	影響部分資訊設備、組織仍可持續營運
二級資安事件	非核心業務受影響、組織仍可持續營運
三級資安事件	部分核心業務受影響
四級資安事件	組織核心業務停擺

3、訂定資安事件紀錄表

發生資安事件時，系統維運人員應記錄各個面向的資安情況於資安事件紀綠表中，以利分析事件內容。資安事件紀錄表之格式及內容可參考《附件1.資安事件紀錄表》。

4、資通系統分級

根據「機密性」、「完整性」、「可用性」、將資通系統分類為「普」、「中」、「高」其中一種等級，當不同等級之系統同時發生資安事件時，應依等級來決定事件處理的優先順序。資通系統之分級可參考《附件6.資通系統分級建議表》。

5、設立專責資安聯絡人員

設立專責資安聯絡人員作為在發生資安事件時和相關單位聯繫之窗口，不論是尋求外部支援或是通報資安事件皆可透過此專責聯絡人進行，以提升

資安事件的應變效率。

6、規劃專業資安教育訓練

資安威脅趨勢與攻擊型態不斷變化，資安人員皆需吸收新的資安知識，對於專責資安事件應處人員應具備之資安技能，「資安技能類型表」提供相應之細項，組織可參考該表與行政院數位發展部之《資通安全專業證照清單》，訂定資安教育訓練計劃。

項次	類型	資安技能
1	網路管理	網路封包分析 網通設備管理
2	資訊系統管理	資料庫應用 Web Server應用 虛擬化平台應用
3	資訊安全	惡意程式分析 事件紀錄分析 資安設備管理
4	程式語言	物件導向程式 資料庫程式 腳本語言

7、規劃資安健檢

資安健檢透過專業人員來執行一系列的檢測，使用自動化工具加上專業分析，以判斷終端設備、網路拓樸、系統架構是否存在問題，而後提出改善建議以提升組織內部的資安量能。目前資安健檢常見的項目包括但不限於：

- 使用者電腦惡意活動檢視
- 核心資通系統內網弱點掃描
- 網路架構檢測
- 網路惡意活動檢視
- 網域主機安全防護檢測

8、建立情資交換與通報管道

加入 TWCERT/CC 或其他資安組織以取得最新的資安情資。

TWCERT/CC 針對網路威脅提出攻擊分析及防護建議，並將其分享給領域成員或會員，以達到資訊安全聯防，增強全體的資安量能。

Email：twcert(at)cert.org.tw

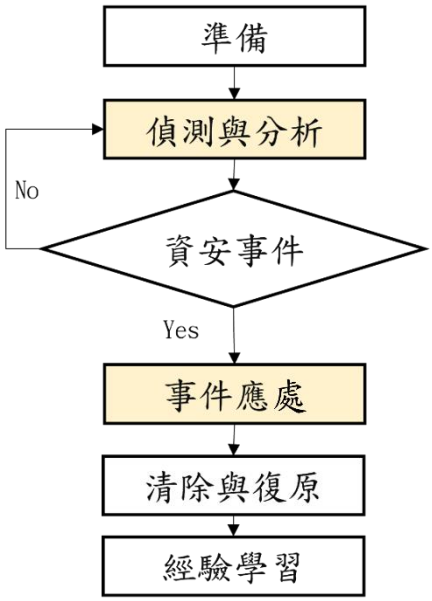
官方網站：請點此進入 TWCERT/CC 官方網站。

完整企業資安事件應變處理指南：

1. 企業資安事件應變處理指南之事前準備

2.1.3、企業資安事件應變處理指南之事中應處

當發生資安事件時，事件處理負責人員必須根據事前的籌劃來應變。在準備階段我們已知道哪些是重要的系統、誰是這些系統的負責人、該使用何種工具。此章節將介紹面臨不同情境的資安事件時可能會有的症狀。本章節的內容對應圖 1 事件處理流程圖中的「偵測與分析」與「事件應處」。



1、資安事件偵測與分析

此階段針對資安事件進行偵測，並藉由流量、Log 監控資訊、系統資源狀態對事件進行分析。表 1 攻擊類型判別對應表列出系統異常症狀及對應的攻擊類型，事件處理負責人員可參考此表來判別可能遭受的攻擊類型。

可能遭受的攻擊類型	症狀	說明
DDoS	1. 服務異常緩慢 2. 伺服器CPU或記憶體使用率飆高 3. 大量不完整的三相交握封包。請參考《附件5.資安應處事中處理工具說明》之第6點 4. 網路流量異常升高	分散式阻斷服務攻擊目的在於目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致使用者無法存取服務。當駭客使用兩個(以上)的殭屍電腦向目標發動「阻斷服務」式攻擊時，稱為分散式阻斷服務攻擊。
勒索軟體	1. 硬碟讀寫率飆升。請參考《附件5.資安應處事中處理工具說明》之第5點 2. 附檔名遭修改 3. 檔案被加密，無法開啟 4. 彈出付款、聯絡方式視窗或以文字檔方式存在桌面	大部分的檔案(註：「文件」是指「檔案」嗎？)會被勒索軟體加密。進行加密時，其特徵為硬碟讀寫率、CPU或記憶體使用率大幅提升。受加密的檔案副檔名會被修改，部分勒索軟體的家族可從此副檔名判別。
惡意程式	1. 彈出視窗廣告畫面 2. 硬碟空間大量損耗 3. 出現可疑工作排程 4. 建立可疑網路連線 5. 瀏覽器首頁重新導向 6. 系統效能緩慢	通常稱為Malware，是malicious software 的組合字。多數的惡意程式的目的為破壞系統、竊取資料或進行其他惡意行為。常見的惡意程式有：木馬、後門程式、間諜軟體、廣告軟體、蠕蟲等。

2、保存數位證據

安事件應變之目的為讓組織能在最短時間內回復正常作業，並保存數位證據供未來採取法律途徑時的證據。即使組織將來不採取法律行動，事件處理負責人員仍應保存數位證據，以利找出入侵的原因並進行修補。底下列出建議保存的資訊；相關的保存工具之使用，請參閱《附件 4.基本數位證據保存工具使用說明》。

- Registry 機碼
- USB 使用紀錄

- Event Log(含 OS、Web、DB、網通設備(Switch、Router 等)、資安設備(IDS、Firewall 等))
- 記憶體資訊
- 系統使用狀態資訊
- 可疑檔案加密封存
- 硬碟映像檔(不在附件內)

3、資安事件應變與處理

在處理事件之前，最重要的便是防止災害擴大，常見的措施如：隔離受感染的主機、系統；中斷受感染的主機、系統之網路。本小節提供對於 DDOS、勒索軟體及惡意程式進行應變處理之建議，並於《附件 5.資安應處事中處理工具說明》說明相關之工具與使用方式。

3.1 DDoS 的應變與處理

- 設置防火牆拒絕外部 ICMP 請求
- 使用具備抵禦 DDoS 的進階防火牆
- 限制流量但不關閉服務
- 設置存取控制清單(ACL)來阻擋可疑 IP 位址的存取
- 允許的情況下增加頻寬以降低攻擊能力
- 網頁服務使用 reCAPTCHA 防止自動連線
- 限制最大連線數量，縮短 idle timeout 時間
- 網路流量清洗

3.2 勒索軟體的應變與處理

- 立即斷開受感染設備與所有網路的連接，無論是有線、無線還是基於

行動網路。

- 監控網路流量並執行防毒掃描以確定是否仍有感染
- 盤點其他可能受影響的設備，並對這些設備執行防毒軟體掃描
- 根據勒索軟體名稱、副檔名等資訊，查找該病毒的類型；在 No More Ransom Project 的網站上，尋找可信任資安單位提供的解密工具。
- 檔案系統進行備份

3.3 惡意程式的應變與處理

- 隔離受感染系統，避免擴散感染
- 阻斷惡意程式嘗試通聯的網路
- 使用 TCPView 偵測網路行為，觀察受感染的系統是否連線至外部惡意伺服器。若是，則將其封鎖。請參考《附件 5.資安應變事中處理工具說明》之第 2 點
- 使用 AutoRuns 查看可疑程式是否於系統開機後自動執行。若是，則將其刪除。請參考《附件 5.資安應變事中處理工具說明》之第 4 點
- 使用 Process Explorer 查看是否有可疑的程式正在執行。若有，則將其刪除。請參考《附件 5.資安應變事中處理工具說明》之第 3 點
- 在主機端和防火牆上關閉所有不必要的 TCP/UDP Port
- 利用 Msert(微軟掃毒軟體)找出可疑檔案，並將其刪除。請參考《附件 5.資安應變事中處理工具說明》之第 1 點

4、通知利害關係人

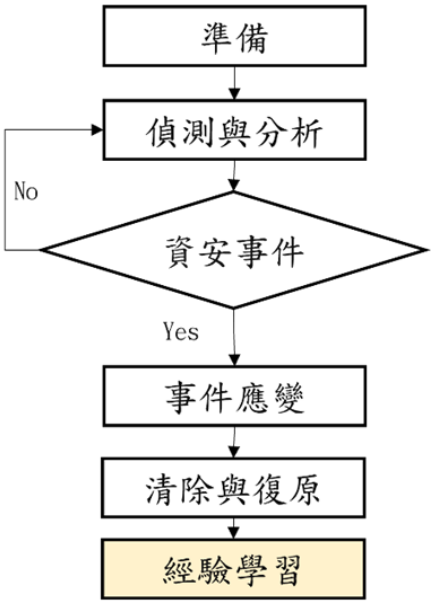
通知各利害關係人，如：客戶、系統使用者、上下游供應商、主管機關等，告知他們目前正面臨何種資安事件、處理的進度、影響的範圍與結果，及預計恢復的時程。

完整企業資安事件應變處理指南：

1. 企業資安事件應變處理指南之事中應處

2.1.4、企業資安事件應變處理指南之經驗學習

資安事件處理完畢後，則進展到事後處置，或稱為經驗學習的階段。此階段的主要目標是「回顧整起資安事件處理過程是否存有須強化之處，使將來面臨類似資安事件時，可更有效的處理」。



在此階段，需考量以下幾個面向：

(1)檢討目前的資安管理制度是否需調整

例如：一般員工的電腦使用者權限是否限縮；防火牆採用的機制是否確實阻擋不必要的服務埠口。

(2)檢視目前的事件處理程序是否合宜

資安的價值在於發生事件後一連串的事件處理與復原，所以發生資安事件並非資安做得不好。每一次的資安事件都是寶貴的經驗，可作為資安人員修改事件處理程序的依據。

(3)資安事件情資分享

建議將攻擊事件資訊通報給 TWCERT/CC，並藉由 TWCERT/CC 將組織內機敏資訊去識別化後，分享給國內外其它組織或情資分享單位，以防範相關攻擊，實現跨域聯防。

(4)檢視其他主機、系統、設備

藉由本次的報告重新檢視組織內部其他主機、系統、設備是否有同樣的弱點。

(5)檢討防護設備是否足夠

透過本次的經驗了解目前缺乏的防護設備，或應設定而未設定的組態，藉此申請設備採購或調整設定。

免責聲明

1.TWCERT/CC（以下簡稱本中心）保留對於本指南所提供之資訊，不另告知而作修正的權利，亦不對任何在本指南上所揭露的資訊精確度、完整性、可靠性或合適性等作擔保聲明，且不負任何明示或默示的保證責任。

2.本中心盡力維護本指南所提供之內容，並確保資料之正確性，但對於內容提供有關之暇疵或不能，或因該暇疵或不能所造成之直接或間接損害，本中心不負任何責任。

3.本指南僅供參考使用，本中心並不擔保其正確性，且用戶明確瞭解並同意，任何因使用、或無法使用本中心指南所造成之直接、間接、偶發、特殊、連帶、或懲戒性損害賠償，包括但不限於獲利損失、資料損失、名譽損害、或其他無形損失等，本中心不負任何損害賠償責任。

完整企業資安事件應變處理指南：

1. 企業資安事件應變處理指南之經驗學習

第 3 章、 國內外重要資安事件

3.1、資安趨勢

2023 年上半年 USB 隨身碟攻擊量再創新高

資安廠商 Mandiant 日前發表研究報告，指出該公司旗下的資安研究人員，近期發現新一波透過 USB 隨身碟發動攻擊的案例，且攻擊量在 2023 年上半年再創歷年新高。

Mandiant 發現的 USB 隨身碟攻擊活動共有兩大系統，其一稱為「Sogu」，疑似與駭侵團體「TEMP.HEX」有關；另一個稱為「Snowydrive」，疑似由另一個駭侵團體「UNC4698」有關，針對亞洲的多家石油與瓦斯公司發動攻擊。

在 Sogu 的攻擊活動方面，Mandiant 指出該駭侵團體鎖定的攻擊目標十分廣泛，遍及美國、法國、英國、義大利、波蘭、奧地利、澳洲、瑞士、中國、日本、烏克蘭、新加坡、印尼和菲律賓。

以行業別來看，遭到 Sogu 攻擊的行業以製藥業和 IT 業最多，均達 11.8%，其次為能源產業（9.4%）、通訊業（9.4%）、醫療業（8.2%）、物流業（7.1%）、非營利組織（5.9%）、零售業（4.7%）、媒體業（4.7%）等。

據 Mandiant 分析，Sogu 使用 DLL order 綁架技術，將一個稱為 Korplug

的惡意軟體酬載載入到 Windows 電腦的記憶體中，然後在登錄檔中新增 Run 機碼，以常駐在電腦中並自動執行，並掃瞄電腦中的 MS Office、PDF 檔案與文字檔，試圖竊取其中的有價值資訊，並上傳到控制伺服器中。

而 Sonwydrive 則會在受害電腦中安裝一個後門，讓駭侵者可以透過 Windows 命令列來載入更多惡意軟體酬載、修改 Windows Registry，竊取檔案內容等。

雖然 USB 隨身碟攻擊的手法已十分老舊，但由於人員資安警覺低，仍有相當的成功率；建議各單位應針對電腦 USB 埠的存取權限提高防範能力，並且加強資安教育訓練，並避免使用任何形式的外部實體儲存裝置。

- 資料來源：
  1. The Spies Who Loved You: Infected USB Drives to Steal Secrets
  2. USB drive malware attacks spiking again in first half of 2023

3.2、新興應用資安

3.2.1、新種無檔案惡意軟體 PyLoose，藏身記憶體內挖掘加密貨幣且難以偵測

資安廠商 Wiz 旗下的資安專家，近日發現一個全新的 Linux 惡意軟體 PyLoose；該惡意軟體衍生自常見的開源加密貨幣挖掘惡意軟體 XMRig，其特色是會藏在受害電腦的記憶體中挖掘加密貨幣，難以透過資安防護工具加以偵測。

據 Wiz 的資安專家指出，這個名為 PyLoose 的惡意軟體是個相對簡單的 Python 指令檔，附有一個預先編譯過的 base64 編碼 XMRig 挖礦程式；XMRig 經常出現在各種以挖掘 Monero 加密貨幣為主的惡意軟體中，會竊取以雲端主機為主的受害電腦 CPU 運算資源來為駭侵者挖掘加密貨幣，獲取不法利潤。

專家說，PyLoose 的特色是不需要在受害主機的磁碟系統中寫入任何檔案，所以各種以檔案數位簽章和惡意軟體特徵碼掃瞄來偵測惡意軟體檔案存在的資安防護工具，就難以偵測出 PyLoose 的存在。

根據 Wiz 的資安專家觀測指出，PyLoose 是資安史上首個以 Python 編寫的無檔案資安攻擊方式，該公司自 2023 年 6 月 23 日起觀測到 PyLoose 的大規模攻擊行動，至今已確認至少 200 個攻擊案例。

Wiz 在報告中指出，駭侵者會先利用一個類似 Pastebin 的網站「Paste.c-net.org」，以 HTTPS GET 要求來取得無檔案的 PyLoose 酬載，然後直接將

PyLoose 載入 Python 的 runtime 記憶體中執行。

Wiz 也在報告中指出，目前尚無法得知利用 PyLoose 來發動攻擊的駭侵者具體身分，且因這個駭侵者採用的手法相當新穎且十分成熟，目前很難研判駭侵者到底是誰。

建議雲端主機的管理者應避免讓主機與服務直接曝露於外網，且應確實做好登入權限防護，包括強式密碼與多重登入驗證；同時對系統指令的執行設定限制。

- 資料來源：
  1. PyLoose: Python-based fileless malware targets cloud workloads to deliver cryptominer
  2. New PyLoose Linux malware mines crypto directly from memory

3.2.2、全新 macOS 惡意軟體 Realst 會竊取加密貨幣錢包內的數位資產

資安研究人員 iamdeadlyz 日前宣布，他發現一個全新的加密貨幣惡意軟體 Realst；該惡意軟體以 Apple 生產的 Mac 電腦為攻擊目標，竊取受害者電腦中加密貨幣錢包中的各種數位資產。

iamdeadlyz 指出，該惡意軟體主要是以假扮成多種區塊鏈遊戲來騙取受害者下載安裝，例如 Brawl Earth、WildWorld、Dawnland、Destruction、Evolion、Pearl、Olymp of Reptiles、SaintLegend 等。

這些遊戲在多個社群媒體或相關論壇都有刊登廣告，駭侵者會利用私訊，假稱傳遞可直接玩這些遊戲的密碼給受害者，讓受害者從駭侵者設立的假網站中下載安裝內含惡意軟體的假遊戲檔案。駭侵者也可以藉由不同的密碼來辨識個別受害者，並且躲避資安防護軟體的追蹤。

一旦受害者安裝了這些假遊戲，安裝程式就會針對受害者使用的作業系統，安裝不同的惡意軟體；Windows 系統會安裝 RedLine Stealer，而這次發現的 Realst 惡意軟體則是針對 macOS 作業系統。

資安研究人員所取得的樣本指出，某些版本的 Realst 惡意軟體甚至能夠支援尚未正式推出，目前僅有測試版的 macOS 14 Sonoma。

據資安廠商 SentinetOne 取得的十多個 Realst 取樣研究報告指出，該惡意軟體會竊取安裝於 macOS 系統上的多種瀏覽器和通訊軟體，例如 Firefox、Chrome、Opera、Brave、Vivaldi、Telegram，以竊取其中儲存或傳遞的機敏

資訊，但都未針對 Safari 進行攻擊。

建議 Mac 使用者應避免自官方 App Store 以外來源安裝 .PKG 檔或 .DMG 檔，以免遭到惡意軟體攻擊。

- 資料來源：
  1. Fake Blockchain Games Deliver RedLine Stealer & Realst Stealer - A New macOS Infostealer Malware
  2. New Realst macOS malware steals your cryptocurrency wallets
  3. Apple Crimeware | Massive Rust Infostealer Campaign Aiming for macOS Sonoma Ahead of Public Release

3.2.3、Lazarus 駭侵團體疑與一起 6,000 萬美元加密貨幣竊案相關

區塊鏈分析師指出，APT 駭侵團體 Lazarus 疑似與近期發生的加密貨幣付款平台 Alphapo 攻擊事件有關；該攻擊事件造成高達 6,000 萬美元的加密貨幣被竊。

Alphapo 是一個集中化的加密貨幣付款平台，服務對象包括多個線上博弈平台、電子商務訂閱等多種網路平台。該服務於 2023 年 7 月 23 日遭到駭侵攻擊，當時估計的被竊加密貨幣總額高達 2,300 萬美元，計有 600 萬美元的 USDT、10.8 萬枚 USDC、1,002 萬美元的 FTN、430 萬美元的 TFL、2,500 美元的 ETH、1,700 美元的 DAI 等。

據指出，上述 Alphapo 被竊的數位資產，都竊自該平台的線上熱錢包；可能是因為該平台的錢包私鑰遭竊所致。

另外也有區塊鏈投資者與分析師指出，Lazarus 另外還竊得 3,700 萬美元的 TRON 與比特幣，所以總共因攻擊取得的數位資產高達 6,000 萬美元之多。

Lazarus 駭侵團體長久以來均以加密貨幣相關駭侵為主要攻擊領域；過去該團體曾經涉及高達 3,500 萬美元的 Atomic 錢包竊案、1 億美元的 Harmony Horizon 攻擊，以及 6.17 億美元的 Axie Infinity 竊案。

該駭侵團體也經常在 LinkedIn 等求職網站，以詐騙的高薪求才廣告招徠，引誘大型加密貨幣業者的員工跳槽，藉以駭入這些受害者的電腦，竊取

其所屬企業的機敏資訊與數位資產。

建議加密貨幣相關業者務必將客戶資金存放在冷錢包中，且應隨時檢測資安防護，以免大筆資金遭竊。

- 資料來源：
  1. PeckShieldAlert @PeckShieldAlert
  2. ZachXBT @zachxbt
  3. Lazarus hackers linked to $60 million Alphapo cryptocurrency heist

3.3、國際政府組織資安資訊

3.3.1、象牙海岸警方會同國際刑警組織，捕獲 OPERA1ER 網路犯罪集團要角

西非國家象牙海岸警方日前會同國際刑警組織（INTERPOL）、非洲刑警組織（AFRIPOL）與資安廠商 Group-IB、資通業者 Orange，以及美國特勤局（US Secret Service）旗下的犯罪調查部門、德國與英國相關單位和多位資安專家的協助之下，合力捕獲大型跨國網路犯罪集團 OPERA1ER 的一名要角，並繼續深入追查。

OPERA1ER 網路犯罪集團又稱為 NXM、DESKTOP Group 和 Common Raven，近年來涉及多起使用惡意軟體、釣魚和商業電子郵件攻擊（Business Email Compromise, BEC）等方式，跨國攻擊非洲、亞洲和拉丁美洲的多家金融機構。

據偵辦單位指出，OPERA1ER 犯罪集團，光在 2022 年的一年之間，就對上述各地 15 個國家的金融機構，發動至少 30 次以上的攻擊活動，得手的不法所得約在 1,100 萬美元到 3,000 萬美元之間。

這場針對 OPERA1ER 的跨國共同司法行動，其代號為「Operation NERVONE」，由象牙海岸警方發動追捕行動，成功逮捕一名該集團的重要人物。目前正在進行進一步的清查。

據報導指出，Group-IB 和 Orange 旗下的 CERT-CC 部門，自 2019 年起就開始追蹤 OPERAT1ER 的不法活動，查出在 2018 到 2022 年之間有 35 次成

功的攻擊活動與該集團有關。

調查也表示，OPERAT1ER 犯罪集團成員均說法語，據信主要在非洲地區活動，主要透過各種開源攻擊工具和如 Metasploit 和 Cobalt Strike 等框架發動攻擊。

鑑於跨國網路攻擊行動日益頻繁且猛烈，建議各國金融機構與各種規模企業均應提高資安防護能力，並特別防範 BEC 等針對商業組織的攻擊行動。

- 資料來源：
  1. Operation Nervone: Group-IB assists INTERPOL-led mission to detain key cybercrime suspect in Côte d'Ivoire
  2. Police arrest suspect linked to notorius OPERA1ER cybercrime gang

3.3.2、CISA 警告美國政府各單位立即修補已遭攻擊的 Android 驅動程式漏洞

美國資安最高主管機關「網路安全暨基礎設施安全局」（Cybersecurity and Infrastructure Security Agency, CISA）近日發布命令，要求美國聯邦政府旗下各單位立即修補一個高危險的 ARM Mali GPU 核心驅動程式執行權限提升漏洞。

CISA 通令修補的漏洞為 CVE-2021-29256，是一個「釋放後使用」（use-after-free）漏洞，駭侵者可操弄受攻擊 Android 系統上的 GPU 記憶體，誘發這個漏洞來提升自身執行權限到最高的 root 等級，即可存取各種裝置上的機資訊。

CVE-2021-29256 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）；CISA 是在 2023 年 7 月 28 日將這個漏洞列入「已知遭濫用漏洞列表」（Known Exploited Vulerabilities Catalog，KEVC）之中。

依 CISA 規定，任何美國聯邦政府旗下單位，都應在新漏洞列入 KEVC 清單後限期應對，包括進行資安修補或其他防範措施，以防止遭駭侵者利用該漏洞發動攻擊。以這個 CVE-2021-29256 而言，美國聯邦政府旗下單位最遲應在 7 月 28 日之完成相關系統的漏洞修補作業。

CVE-2021-29256 早在 2021 年 3 月 26 日由 ARM 推出更新。Google 於 2023 年 7 月發表的 Android 安全公告中，則提到該漏洞可能已經遭到駭侵者用於攻擊。

雖然 CISA 發表的 KEV 資安更新通令僅對美國聯邦政府旗下單位有約束力，但建議各公私單位依照 CISA 通報進行各種系統的資安更新。

- 資料來源：
  1. Mali GPU Driver Vulnerabilities
  2. Android 安全性公告 - 2023 年 7 月
  3. CISA warns govt agencies to patch actively exploited Android driver

3.3.3、美國計畫針對安全性較高的智慧裝置推出網路安全認證標章「Cyber Trust Mark」

美國計畫推出一個名為「網路安全信任標誌」（Cyber Trust Mark）的資安防護認證產品標章，供通過認證的網站標示，以協助美國消費者在選購連網裝置時，可以依該標章選購安全性較高、對抗駭侵攻擊韌性較強的產品。

Cyber Trust Mark 標章的提案，是由美國聯邦通訊委員會（Federal Communication Commission, FCC）提出，並接受各方建議。這個標章預計在明年正式上路，供各種智慧連網製造商申請使用。

在提案中規定，要獲得 Cyber Trust Mark 標章的產品，必須符合美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）提出的資安規範標準，包括預設使用強式密碼、資料保護、軟體或韌體更新、事故偵測能力等標準。

在由白宮發表的一份新聞稿中指出，FCC 推出 Cyber Trust Mark 的目的，除了要保護美國消費大眾在使用各種連網裝置時的安全性外，更要提高這類裝置的一般資安保護水準。

這個標章預計將適用於各類連網裝置，包括智慧家電如冰箱、微波爐、電視、空調系統、健身追蹤器材等等。目前已有多家智慧連網家電暨裝置大廠宣布加入這個標章系統，包括 Amazon、Best Buy、Google、LG Electronics USA、Logitech、Samsung Electronics 等。

待 Cyber Trust Mark 上路後，符合標準的產品將可貼上專屬標章，並列表

於一份可公開查閱的產品清單中，以供消費者選購產品時參考之用。

建議政府單位、廠商與相關資安單位，可參考該標章的標準與做法，推動在國內市場販售的連網裝置也有同類標示，可供消費者參考，並強化社會大眾的資安意識。

- 資料來源：
  1. Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers
  2. U.S. preparing Cyber Trust Mark for more secure smart devices

3.3.4、烏克蘭警方破獲大型機器人機房，查獲 15 萬張 SIM 卡

烏克蘭警方的網路警察部門，日前宣布破獲一個大型機器人機房，除了搜索超過 12 處地點、250 台以上 GSM 閘道器、逮捕 100 人以上之外，還查獲 15 萬張 SIM 卡。

烏克蘭警方說，這個機器人機房是用以在烏克蘭發送俄羅斯入侵烏克蘭正當性的政治軍事宣傳之用，同時也涉及多起詐騙案件。

烏克蘭警方一共在 Vinnytsia、Zaporizhzhia 和 Lvivand 同步執行 21 個搜索行動，緝獲大量電腦設備、手機、250 個以上 GSM 閘道器，以及多家電信業者近 15 萬張 SIM 卡。

烏克蘭警方說，駭侵者使用特殊設備和軟體，利用這些 SIM 卡門號，在多個社群網站大量註冊數千個帳號，並以這些帳號來發送違反烏克蘭法律的內容，包括政治軍事宣傳、假訊息、詐騙攻擊，並且傳送烏克蘭公民的個人資料，威脅烏克蘭人民的人身與財產安全。

這並不是烏克蘭首次破獲用來傳遞假消息和政治軍事宣傳的機房，2022 年 8 月和 9 月共破獲兩處機房，其中一處有多達 100 萬台假帳號機器人。這些被破獲的機房位於 Kharkiv、Cherkasy、Ternopil 和 Zakarpattia。

在過去多次假消息攻擊中，烏克蘭總統澤倫斯基也成為攻擊目標，有多支利用深偽技術的假訊息影片，透過這些機器人網路在 Facebook 和其他熱門社群網路上散布，甚至連烏克蘭境內的廣播電台也曾遭挾持並用以發送假訊

息。

建議政府單位加強一般民眾對假訊息的媒體識讀能力，並加強偵測各種境內境外的假訊息活動；平台應強化對於帳號註冊的管控與協同貼文限制。

- 資料來源：
  1. Кіберполіція викрила організаторів ботоферм, які поширювали ворожу пропаганду та займалися інтернет-шахрайствами
  2. Ukraine takes down massive bot farm, seizes 150,000 SIM cards

3.4、社群媒體資安近況

3.4.1、Mastodon 伺服器遭駭侵者透過嚴重 TootRoot 漏洞進行攻擊

開源且免費的去中心化社群平台 Mastodon 日前緊急發表資安修補更新，修復 4 個資安漏洞；其中包含一個嚴重的資安漏洞 CVE-2023-36460；駭侵者可透過特製的媒體檔案，在伺服器上任意新增檔案。

發現這 4 個資安漏洞的是獨立資安檢測廠商 Cure53，在 Mozilla 的要求之下檢視 Mastodon 的源碼後，發現這四個漏洞。

其中最嚴重的是 CVE-2023-30460 這個漏洞；該漏洞已命名為「TootRoot」，存於 Mastodon 的媒體處理相關程式碼中；駭侵者可透過 toots（相當於 Twitter 上的 Tweet）夾帶特製的媒體檔案，誘發這個錯誤，進而攻陷含有此漏洞的 Mastodon 伺服器，包括對其進行服務阻斷攻擊（Denial of Service, DoS）或是在該伺服器上執行任意程式碼。

駭侵者除了可以完全控制受攻擊的 Mastodon 伺服器外，也能竊取伺服器上的所有資料，包括使用 Mastodon 社群服務的使用者資訊在內。

另一個嚴重漏洞是 CVE-2023-36459，存於 Mastodon 的 oEmbed 預覽卡片中，屬於跨網站指令碼攻擊（Cross-site scripting, XSS）。攻擊者可以利用這個漏洞跳過系統對輸入 HTML 碼的檢查過程，並可以用來竊取其他使用者的帳號、假冒其他使用者，或存取使用者的機敏資訊。

建議 Mastodon 的伺服器管理者，應立即套用更新，升級到 3.5.9、4.0.5

與 4.1.3 或更新版本，以修補這 4 個漏洞，避免遭駭侵者利用已知漏洞進行攻擊。

- 資料來源：
  1. Security Advisories
  2. Critical TootRoot bug lets attackers hijack Mastodon servers

3.4.2、WordPress 外掛程式 AIOS 被發現使用明文記錄密碼

一個名為 All-in-One Security（AIOS）的 WordPress 資安防護外掛程式，近日遭到用戶發現，其運作方式以明文方式來儲存用戶輸入的密碼，而未經加密儲存；這可能導致使用者的資安曝於風險之下。

All-in-One Security（AIOS）是由軟體開發廠商 Updraft 開發的 WordPress 網站專用資安防護外掛程式，可以提供 web application 的防火牆、內容防護、登入安全等額外的資安防護功能，以防殭屍網路機器人或暴力試誤法的攻擊。

約在三個多星期前，有位 All-in-One Security（AIOS）的使用者在 WordPress.org 的支援討論區中發文指出，他發現 All-in-One Security（AIOS）v5.19 不只會把使用者的登入記錄寫入到 aiowps_audit_log 這個用來記錄用戶登入、登出、登入失敗等事件的資料表中，更會以明文方式記錄用戶輸入的密碼。

該用戶在發文中也強調，這種做法已經明顯違反 NIST 800-63 3、ISO 27000、GDPR 等資安規範或法規。

All-in-One Security（AIOS）的開發廠商 Updraft 在看到相關貼文後，先是以該問題是一個已知的錯誤（a known bug）來回應，但並未立即承諾具體的修正時間和做法；雖然 Updraft 隨即提供開發中版本供使用者下載，但使用者回報指出新的開發版並未解決問題，也沒有刪除記錄在資料表中的密碼。

不過 Updraft 在 7 月 11 日時提供了新版的 All-in-One Security（AIOS）v5.2.0，自此版本起不再以明文儲存用戶輸入的密碼，同時會自資料表中刪除先前儲存的密碼。

建議 All-in-One Security（AIOS）的用戶應立即將該外掛程式升級至 V5.2.0 版。

- 資料來源：
  1. Cleartext passwords written to aiowps_audit_log
  2. All-In-One Security (AIOS) WordPress Security Plugin Release 5.2.0

3.5、行動裝置資安訊息

3.5.1、Google Play Store 中的 2 個 Android App 會竊取用戶資料，已下載 150 萬次以上

資安廠商 Pradeo 旗下的資安研究人員，近日發現有 2 個上架於 Google Play Store 中的 Android App，會暗中竊取用戶手機中的多種資料，並傳送回伺服器。這兩個 App 的下載次數合計高達 150 萬次。

這兩個 App 分別名為「File Recovery & Data Recovery」和「File Manager」，都是由同一個署名為「wang tom」的開發單位上架於 Google Play Store，都是屬於檔案管理型的應用軟體。前者的下載安裝次數達 100 萬次，後者則有 50 萬次之多。

Pradeo 的應用軟體行為分析引擎，發現這兩個 App 儘管在其隱私權與 App 所需權限中聲明該兩支 App 不收集使用者資料，但實際上卻會自使用者的手機中竊取下列機敏資訊，而且未曾告知使用者：

- 裝置記憶體、連線的 Email 通訊錄和社群平台上的用戶通訊錄；
- 以該 App 管理或復原的圖片、音訊和影片檔案；
- 使用者即時所在地資訊；
- 行動電話國碼；
- 網路供應商名稱；
- SIM 卡供應商的網路代碼；

- 作業系統版本號碼；
- 手機廠牌與型號；

Pradeo 也說，這兩個 App 如同其他多種 Android 惡意軟體，會將自己的圖示自手機主畫面中隱藏起來，讓使用者難以發現並且刪除；Pradeo 也指出這兩個 App 同時也會濫用使用者授與的執行權限，將自己放在背景中，使用者一開機就會自動執行。

這兩個 App 目前已遭 Google 下架。

建議 Android 手機使用者即使在官方的 Google Play Store 中下載安裝軟體，也應提高警覺，仔細閱讀其他使用者的意見回饋。如遇要求過多權限的 App，應拒絕授與並立即刪除。

- 資料來源：
  1. Two spyware tied with China found hiding on the Google Play Store
  2. Apps with 1.5M installs on Google Play send your data to China

3.5.2、Apple 修復已用於攻擊的全新 0-day 漏洞 CVE-2023-37450

Apple 近期釋出一個資安更新，用以修復已證實遭駭侵者用於攻擊 iPhone、iPad 和 Mac 裝置的 0-day 漏洞 CVE-2023-37450。

這個漏洞存在用於 iPhone、iPad 與 Mac 的 WebKit 瀏覽器核心之中，駭侵者可透過特製的網頁內容，來觸發 CVE-2023-37450 的發生，藉以執行任意程式碼。

該漏洞係由一位匿名的資安研究人員通報，Apple 在該公司發表的資安通報中指出，該公司已經知悉本漏洞已遭駭侵者積極用於攻擊活動之中。

此外，Apple 最新推出的資安更新，也同時解決另一個亦可能已遭駭侵者大規模用於攻擊的 0-day 漏洞 CVE-2023-38606；該漏洞存於作業系統的核心之內，駭侵者可以利用這個漏洞來竄改敏感的作業系統核心狀態。

針對 CVE-2023-38606，Apple 也在資安通報中指出，該公司業已獲悉有駭侵者利用此漏洞攻擊作業系統版本仍在 iOS 15.7.1 之前舊版本的 iOS 裝置。

資安廠商卡巴斯基旗下的首席資安研究員 Boris Larin 也針對 CVE-2023-38606 發表推文指出，有駭侵團體使用該漏洞，透過特製的 iMessage 內容來觸發此漏洞，配合其他攻擊方式來布署一個名為 Triangulation 的惡意軟體。

Apple 這次發表的資安更新，係針對 macOS Ventura 13.4、iOS/iPad OS 16.5、tvOS 16.5、watchOS 9.5、Safari 16.5 等舊版本發行，加強其邊界檢查、

輸入驗證與記憶體管理。

由於受兩個 0-day 漏洞的影響範圍很大，建議所有 iPhone、iPad 與 Mac 使用者均應立即更新到最新版本作業系統。

- 資料來源：
  1. About the security content of macOS Ventura 13.5
  2. Dissecting TriangleDB, a Triangulation spyware implant
  3. Apple fixes new zero-day used in attacks against iPhones, Macs

3.5.3、APT41 駭侵團體利用 WyrmSpy、DragonEgg 間諜軟體攻擊 Android 使用者

資安廠商 Lookout 指出，進階持續性威脅團體 APT41 近期利用兩個間諜軟體 WyrmSpy 和 DragonEgg，鎖定 Android 手機使用者發動攻擊。

APT41 過去長期針對美國、亞洲和歐洲各國的各種目標發動攻擊，曾受 APT41 駭侵攻擊的單位包括軟體開發、硬體製造、政策智庫、電信通訊、大專院校與外國政府等等。

Lookout 是在 2017 年時首先發現 WyrmSpy，並在 2021 年初發現 DragonEgg；近期則是在 2023 年 4 月再次發現其攻擊活動。這兩個 Android 惡意軟體都具有強大的資料竊取能力。

據 Lookout 指出，WyrmSpy 的感染方式主要是以偽裝為 Android 系統維護軟體為主，而 DragonEgg 則會偽裝為第三方鍵盤軟體或即時通訊軟體，且透過各種手段來避免遭到防毒防駭軟體的偵測。

由於 WrymSpy 和 DragonEgg 使用相同的 Android 數位簽章，因此可以推測這兩個惡意軟體係為同一來源。Google 也指出，目前尚未在 Google Play Store 中發現任何 App 含有這兩個惡意軟體。

據 Lookout 發表的報告指出，APT41 除了會入侵政府單位竊取情報之外，也會針對私人企業發動駭侵攻擊，以取得財務上的不法收入。而過去 APT41 主要是利用各種 Web App 和曝露於外網裝置中的漏洞來發動攻擊，但近年來也開始利用如 WyrmSpy 和 DragonEgg 之類的惡意軟體來攻擊 Android

裝置。

建議 Android 使用者應避免安裝來路不明的 apk 檔案，apk 檔案為 Adnroid 惡意軟體的來源之一。

- 資料來源：
  1. Lookout Attributes Advanced Android Surveillanceware to Chinese Espionage Group APT41
  2. APT41 hackers target Android users with WyrmSpy, DragonEgg spyware

3.6、軟體系統資安議題

3.6.1、近 40% Ubuntu 系統含有權限提升與任意程式碼執行的資安漏洞

資安廠商 Wiz 旗下的資安研究人員，近期在廣受歡迎的 Linux 發行版本 Ubuntu 的核心中發現兩個漏洞，可讓未擁有高等級權限的本機使用者提升其執行權限，並且執行任意程式碼。

這兩個漏洞分別為 CVE-2023-32629 和 CVE-2023-2640。CVE-2023-2640 是個存於 Ubuntu Linux 核心記憶體管理子系統中，一個不適當的權限檢查機制造成的權限提升漏洞，能夠存取本機的駭侵者，可以利用該漏洞來提升執行權限。

另一個漏洞 CVE-2023-32629 也存於 Ubuntu Linux 核心記憶體管理子系統中，在存取 VMA 時可能形成競爭狀況並導致記憶體發生「釋放後使用」（use-after-free）問題，使可以存取本機資源的駭侵者藉以執行任意程式碼。

CVE-2023-2640 的 CVSS 危險程度評分較高，為 7.8 分（滿分為 10 分），其危險程度評級為「高」（high）；而 CVE-2023-32629 的 CVSS 分數略低，為 5.4 分，其危險程度評級為「中」（medium）。

資安研究人員是在研究 Ubuntu Linux 在實作 OverlayFS 檔案系統發生的不相容問題時，發現這兩個漏洞。過去在 2018 年之前的 Ubuntu Linux 發行版，在執行 OverlayFS 時並不會發生任何問題，但在 2019 年和 2022 年，Linux 核心專案進行部分變動，就導致在 Ubuntu Linux 核心在執行 OverlayFS

時發生上述兩個漏洞。

由於 Ubuntu 的使用層面極廣，Wiz 的研究人員估計約有 40% 的 Ubuntu 系統含有此二漏洞；Ubuntu 基金會也已推出資安更新，用戶應立即套用。

Ubuntu 基金會也已針對這兩個漏洞與其他資安漏洞推出資安更新，建議用戶應立即套用。

- 資料來源：
  1. GameOver(lay): Easy-to-exploit local privilege escalation vulnerabilities in Ubuntu Linux affect 40% of Ubuntu cloud workloads
  2. USN-6250-1: Linux kernel vulnerabilities

3.6.2、資安廠商分析 2000 萬筆惡意軟體記錄，發現近 38 萬筆企業登入資訊遭竊

資安廠商 Flare 分析近 2000 萬筆求售資訊竊盜惡意軟體的記錄檔後，發現有近 38 萬筆企業用於各種雲端服務的登入資訊遭到竊取。

Flare 分析的惡意軟體記錄檔，係取自駭侵者在暗網上的駭侵相關論壇與 Telegram 駭侵討論頻道中出售的大量記錄資料，因而發現企業登入資訊大量遭竊的情形。

Flare 分析的資訊竊取惡意軟體包括 Redline、Raccoon、Titan、Aurora、Vidar 等，這些惡意軟體以出租的方式提供給駭侵分子使用，並透過各種方法引誘用戶下載，不但對個人使用者造成資安威脅，也對企業造成很大的資安風險。駭侵者可以利用這些竊得的登入資訊，攻擊企業使用的 VPN、RDP、CRM 系統，進行更大的破壞。

Flare 指出，這些惡意軟體主要攻擊企業使用者，並且竊得許多主流企業用雲端系統的登入資訊；Flare 取得的記錄檔數量如下：

- 179,000 筆 AWS Console 登入資訊；
- 2,300 筆 Google Cloud 登入資訊；
- 64,500 筆 DocuSign 登入資訊；
- 15,500 筆 QuickBooks 登入資訊；
- 23,000 筆 Salesforce 登入資訊；

- 6,600 筆 CRM 登入資訊。

Flare 也表示，這些資訊中有 74% 是取自 Telegram 頻道，其餘約 25% 則來自駭侵論壇上的賣場，如「Russian Market」。

另外 Flare 也發現有 20 萬筆資訊竊取記錄內含 OpenAI 的登入資訊，這表示企業使用 OpenAI 時輸入或取得的相關資訊，也面臨遭駭侵者利用的風險。

建議企業應全面加強各種資安防護能力，並強化員工資安意識，以免成為資安破口，導致惡意軟體有機可趁。

- 資料來源：

1. Report - Stealer Logs & Corporate Access
2. Over 400,000 corporate credentials stolen by info-stealing malware

3.7、軟硬體漏洞資訊

3.7.1、三十萬台以上 Fortinet 防火牆仍未修補嚴重漏洞 CVE-2023-27997

資安廠商 Bishop Fox 日前發表研究報告，指出該公司旗下研究人員發現，外網上仍有三十萬台以上由 Fortinet 生產的 FortiGate 防火牆裝置，仍未完成嚴重漏洞 CVE-2023-27997 的修補，可能導致駭侵者遠端執行任意程式碼。

CVE-2023-27997 漏洞可讓駭侵者在未經授權的情形下，透過曝露在 Internet 上的 Fortinet 網通裝置 SSL VPN 設定用 web 介面來遠端執行任意程式碼。該漏洞的 CVSS 危險程度評分高達 9.8 分（滿分為 10 分），其危險程度評級亦為最高等級的「嚴重」（Critical）等級。

CVE-2023-27997 是在今年六月中旬時發現，Fortinet 在漏洞情報公開之前就已備妥修補程式，除了提醒用戶及早更新以修補漏洞外，也指出該漏洞已遭駭侵者大規模濫用於資安攻擊上。

在 Fortinet 推出修補程式的半個多月後，Bishop Fox 的研究人員利用 Shodan 搜尋引擎，還是找到了有超過三十萬台以上的 Fortinet 設備，不但曝露在外部網路，而且仍未更新到最新版的韌體，可能成為駭侵攻擊的目標。

Bishop Fox 甚至還發現不少曝露於 Intetnet 上的 Fortinet 設備長達 8 年以上均未套用任何更新，其中有部分裝置仍在執行已於 2022 年 9 月停止支援的舊版 FortiOS 6。

Fortinet 於 2023 年 6 月 11 日針對該漏洞推出 FortiOS 新版韌體 6.0.17、6.2.15、6.4.13、7.0.12、7.2.5 版。

- CVE 編號：CVE-2023-27997
- 影響產品(版本)：Fortinet 各式 Fortigate 防火牆產品。
- 解決方案：Fortigate 使用者應立即將產品韌體更新至 6.0.17、6.2.15、6.4.13、7.0.12、7.2.5 版。

- 資料來源：
  1. FortiOS & FortiProxy - Heap buffer overflow in sslvpn pre-authentication
  2. CVE-2023-27997 Is Exploitable, and 69% of FortiGate Firewalls Are Vulnerable
  3. 300,000+ Fortinet firewalls vulnerable to critical FortiOS RCE bug

3.7.2、Cisco 發表資安漏洞 CVE-2023-20185 警訊，可讓駭侵者竊取加密內部傳遞資訊

全球網通產品大廠 Cisco 日前發表資安漏洞警訊，指出該公司部分網通產品內含一個高危險性漏洞 CVE-2023-20185，可能導致駭侵者在未經授權的情形下，讀取甚至竄改網站之間相互傳輸的加密資訊。

該 CVE-2023-20185 漏洞存於 Cisco Nexus 9000 資料中心系列的骨幹交換器，詳細受影響機種為 Cisco Nexus 9332C、9364C 與 9500，且交換器需處於 ACI 模式，設定為多網站拓樸架構，且已啟用 CloudSec 加密功能，並執行 firmware 14.0 之後的版本。

Cisco 指出，該漏洞是因為在實作 CloudSec 加密時的編碼出現問題，處於 on-path 位置的駭侵者將可利用此漏洞來攔截網站間的加密通訊，甚至予以解碼、竄改。

CVE-2023-20185 的 CVSS 危險程度分數高達 7.4 分（滿分為 10 分），危險程度評級為「高」；到目前為止，Cisco 尚未針對這個漏洞發表更新版本的韌體。

Cisco 指出，使用受此漏洞影響裝置的用戶，可以關閉 CloudSec 相關功能，以暫時解決此一漏洞；使用者可依 Cisco 公布的指引，在不同機型上檢查是否已開啟 CloudSec 功能並將其停用。

另外 Cisco 也指出，目前尚未發現有駭侵者利用 CVE-2023-20185 漏洞發動大規模駭侵攻擊的跡象。

- CVE 編號：CVE-2023-20185
- 影響產品(版本)：Cisco Nexus 9332C、9364C 與 9500。
- 解決方案：依照 Cisco 提供的指引，在不同機型上檢查是否已開啟 CloudSec 功能並將其停用。

- 資料來源：
  1. Cisco ACI Multi-Site CloudSec Encryption Information Disclosure Vulnerability
  2. Cisco warns of bug that lets attackers break traffic encryption

3.7.3、Microsoft 推出 2023 年 7 月 Patch Tuesday 每月例行更新修補包，共修復 132 個資安漏洞，內含 6 個 0-day 漏洞

Microsoft 日前推出 2023 年 7 月例行資安更新修補包「Patch Tuesday」，共修復 132 個資安漏洞；其中含有 6 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 132 個，較上個月（2023 年 6 月）的 78 個資安漏洞多了很多；而在這 132 個漏洞中有多達 6 個是屬於已知遭到駭侵者用於攻擊的 0-day 漏洞，另外還有 37 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：

- 權限提升漏洞：33 個；
- 資安防護功能略過漏洞：13 個；
- 遠端執行任意程式碼漏洞：37 個；
- 資訊洩露漏洞：19 個；
- 服務阻斷（Denial of Service）漏洞：22 個；
- 假冒詐騙漏洞：7 個；
- Edge -Chromium 漏洞：0 個。

本月的 Patch Tuesday 有 6 個已遭大規模濫用的 0-day 漏洞：

第一個是 CVE 編號為 CVE-2023-32046 的 Windows MSHTML Platform 權限提升漏洞；該漏洞存於 Windows MSHTML 系統之中，可讓駭侵者以 EMail 或惡意網站，透過特製的檔案將自身執行權限提升執行受影響軟體用戶相同的等級。

第二個值得注意的漏洞是 CVE-2023-32049，是存於 Microsoft SmartScreen 中的資安防護功能略過漏洞。駭侵者可利用此漏洞，讓用戶自網路下載或開啟可能有資安風險的檔案時，系統不會顯示資安警訊提示。

- CVE 編號：CVE-2023-32046、CVE-2023-32049 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. Windows MSHTML Platform Elevation of Privilege Vulnerability
  2. Windows SmartScreen Security Feature Bypass Vulnerability
  3. Microsoft July 2023 Patch Tuesday warns of 6 zero-days, 132 flaws

3.7.4、1.5 萬台以上 Citrix 伺服器易遭駭侵者以 CVE-2023-3519 攻擊

非營利資安組織 Shadowserver Foundation 旗下的資安研究人員，近日發現有至少 15,000 台的 Citrix NetScaler ADC 與 Gateway 伺服器，內含可能導致駭侵者遠端執行任意程式碼的嚴重漏洞 CVE-2023-3519，且曝露在對外網路上，風險極高。

根據 Shadowserver Foundation 提供的報告指出，含有 CVE-2023-3519 漏洞且曝露於外網的伺服器，以分布在美國境內的裝置數量最多，達到 5,700 台，其次為德國（1,500 台）、英國（1,000 台）、澳大利亞（582 台）、瑞士（509 台）、加拿大（509 台）、法國（451 台）、中國（402 台）、荷蘭（358 台）、瑞典（308 台）、義大利（290 台）、日本（253 台）等。

CVE-2023-3519 最早是在 2023 年 7 月初時因某駭侵者在某駭侵論壇上張貼一則關於 Citrix 0-day 漏洞廣告而曝光；該漏洞可讓駭侵者在沒有獲得授權的情形下，遠端執行任意程式碼，且其 CVSS 危險程度評分高達 9.8 分（滿分為 10 分）。

受此漏洞影響的 Citrix 裝置與版本相當多，Citrix 也在 7 月 18 日針對 CVE-2023-3519 推出了更新版韌體，以修復該漏洞。甚至美國資安主管機關 CISA 也在上周明令政府單位須限期更新此漏洞。

不過按照 Shadowserver Foundation 的報告，全球顯然還有許多內含此漏洞尚未更新的裝置，且都曝露於對外網路上。

- CVE 編號：CVE-2023-3519
- 影響產品(版本)：NetScaler ADC 與 NetScaler Gateway 13.1-49.13 與先前版本；其他產品請參閱 Citrix 發布之資安通報。
- 解決方案：建議立即依原廠指示升級到指定版本韌體，相關裝置也應受防火牆之保護，避免曝露於外部網路連線。

- 資料來源：
  1. Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467
  2. Shadowserver @Shadowserver
  3. Over 15K Citrix servers vulnerable to CVE-2023-3519 RCE attacks

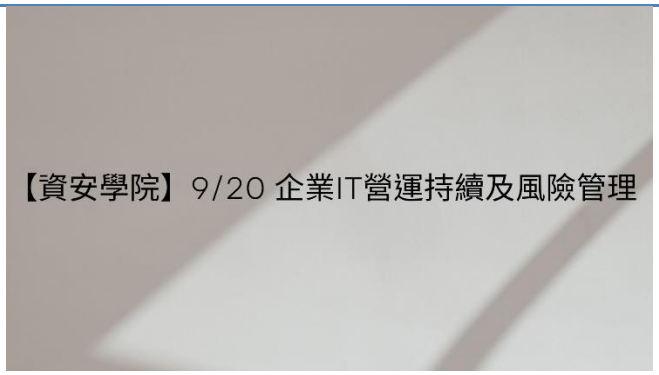
第 4 章、 資安研討會及活動

【2023 年數位應用週】08/23 資安有韌性，企業會更好 論壇直播	
活動時間	**2023/08/23 13:50 ~ 16:30**
活動地點	**線上**
活動網站	**https://digi.cisa.tw/forum17.htm**
活動概要	 **主辦單位：中華民國資訊軟體協會** 資安一直是企業面臨的重大挑戰，尤其在這個數位化快速發展的時代。威脅逐漸變得更加複雜多樣化，資訊安全攸關企業的業務連續性、客戶信任和競爭優勢。因此，企業必須保持警覺並持續提升資安韌性，以應對不斷變化的威脅環境。本次「資安有韌性，企業會更好」將聚焦於資安領域的最新趨勢和關鍵議題，探討如何在數位轉型的浪潮中建立具有韌性的資安策略，以使企業能夠更好地應對不斷演進的數位風險。 聯絡窗口： 02-2553-3988 分機 629　林資深專員 kash@cisanet.org.tw 報名截止： 2023-09-02 (線上報名後，即可免費參加)

人工智慧將如何改變未來工作？	
活動時間	**2023 年 08 月 23 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/20230823/**
活動概要	 **主辦單位：TWNIC、NII、TWIGF** 今年 5 月，包括奧斯卡獲獎導演及諸多好萊塢影視編劇們，集結在 Netflix 工作室外頭舉牌抗議，大力反對 AI 生成劇本；於此同時，在華語界 AI 孫燕姿早已在網路影音平台爆紅，翻唱了數首百萬點閱率的歌曲。AI 掀起對未來工作的改變，絕不只是在影視領域而已。 美國人工智慧權威 Ben Goertzel 在一場訪談中提到，AI 可能在未來幾年內取代 80% 的人類工作；他也提醒，「未來」就是數年後，而非數十年。另一個聳動預測則來自於高盛：如 ChatGPT 這類的流行 AI 工具背後技術，未來將自動化相當於 3 億個全職工作。而 OpenAI 和賓州大學的研究人員也預估，八成的美國勞工有機會看到至少 10% 的任務受影響，此處的受影響可能是變得更好或變得更糟，甚至失業。 從大師與專家們的推測中，AI 看似非常可能破壞勞動力市場。因為自動化系統有機會取代部甚至剝奪一部分人的工作權。但也有主張認為，AI 在像是護理、長照、家務等原本就相對不受人青睞的工作類型中，可扮演很好的角色。此外，AI 還有可能創造新的工作機會。 至於 AI 會如何改變人類的專業價值或勞動力市場？我們又該如何面對 AI 對勞動公平性產生的衝擊？有沒有可能利用 AI 來促進職場中的

	包容性？目前可能沒有人可以回答所有問題，但這個答案與 AI 如何被設計、規範與使用或許有很大的關連性。此亦為本場活動嘗試探索的主題。

【資安學院】9/7 弱點修補技巧（VMS 弱點管理系統）	
活動時間	**2023/09/07 13:30 ~ 17:30**
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/3961**
活動概要	 **主辦單位：中華民國資訊軟體協會** 不論社交工程演練、弱點掃描、滲透測試等資安服務，目的皆是強化資安體質，在資訊安全管理的作業中，針對資訊資產的定期性的弱點評估已經是必要的日常工作。透過有效的弱點管理作業，可大幅降低企業資訊資產發生的潛在風險。 本課程將教導學員如何針對發現系統弱點進行修補技巧，如果分析弱點掃描工具結果並判讀是否為誤判、並強化公司弱點管理是一個持續進行的過程，方便追蹤管理弱點修補情形，本課程將帶領您學習如何修正發現弱點、並依系統環境修補技巧。 聯絡窗口： 02-2553-3988 分機 388　廖資深專員 security@cisanet.org.tw 報名截止： 2023-09-02 費用：原價 4,400/人、早鳥價 4,000/人、軟協會員 3,800/人 費用含稅、教材及完課證明

【資安學院】9/20 企業 IT 營運持續及風險管理	
活動時間	**2023-09-20 09:30 ~ 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/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 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 報名截止： 2023-09-15

第 5 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：

慧智科技 SmartBPM.NET - Use of Hard-Coded Credentials - 1	
TVN / CVE ID	TVN-202307004 / CVE-2023-37286
CVSS	9.8 (Critical)
影響產品	SmartBPM.NET 6.70
問題描述	SmartBPM.NET 使用固定的 machine key，遠端攻擊者不須權限，可以利用 ViewState 進行反序列化攻擊，執行任意程式碼。
解決方法	請聯繫慧智科技詢問相關修補建議
公開日期	2023-07-10
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7221-438c6-3.html

英福達科技 電子公文系統 - Arbitrary File Upload	
TVN / CVE ID	TVN-202307007 / CVE-2023-37289
CVSS	9.8 (Critical)
影響產品	電子公文系統版本 22547、22567
問題描述	英福達科技之電子公文系統上傳功能未對上傳檔案進行檢查限制，導致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	請聯繫英福達科技詢問相關修補建議
公開日期	2023-07-17
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7225-cef32-3.html

桓基科技 HGiga iSherlock - Command Injection	
TVN / CVE ID	TVN-202307010 / CVE-2023-37292
CVSS	9.8 (Critical)
影響產品	HGiga iSherlock (包含 MailSherlock, SpamSherock, AuditSherlock); iSherlock 4.5: iSherlock-user < 4.5-174 ; iSherlock 5.5: iSherlock-user < 5.5-174
問題描述	桓基科技 iSherlock 個人化設定介面 存在 Remote Command Execution 弱點。未登入的攻擊者於系統頁面參數注入系統指令後，即可執行系統任意指令，進行任意系統操作或中斷服務。
解決方法	更新 iSherlock-user 套件至 4.5-174(MSR45) 或 5.5-174 (MSR55) 或更新版本
公開日期	2023-06-16
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7239-8fc29-3.html

ASUS RT-AX56U V2 & RT-AC86U - Format String -1	
TVN / CVE ID	TVN-202307001 / CVE-2023-35086
CVSS	9.8 (Critical)
影響產品	RT-AX56U V2: 3.0.0.4.386_50460; RT-AC86U: 3.0.0.4_386_51529
問題描述	ASUS RT-AX56U V2 與 RT-AC86U 存在 Format String 漏洞，do_detwan_cgi 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-AX56U V2: 更新至 3.0.0.4_386_51598; RT-AC86U: 更新至 3.0.0.4.386_51915
公開日期	2023-07-17

相關連結	https://www.twcert.org.tw/newepaper/cp-151-7240-a5f96-3.html

ASUS RT-AX56U V2 & RT-AC86U - Format String - 2	
TVN / CVE ID	TVN-202307002 / CVE-2023-35087
CVSS	9.8 (Critical)
影響產品	RT-AX56U V2: 3.0.0.4.386_50460 與 RT-AC86U: 3.0.0.4_386_51529
問題描述	ASUS RT-AX56U V2 與 RT-AC86U 存在 Format String 漏洞，cm_processREQ_CHANGED_CONFIG 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-AX56U V2: 更新至 3.0.0.4_386_51598; RT-AC86U: 3.0.0.4.386_51915
公開日期	2023-07-17
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7249-ab2d1-3.html

第 6 章、 2023 年 7 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。

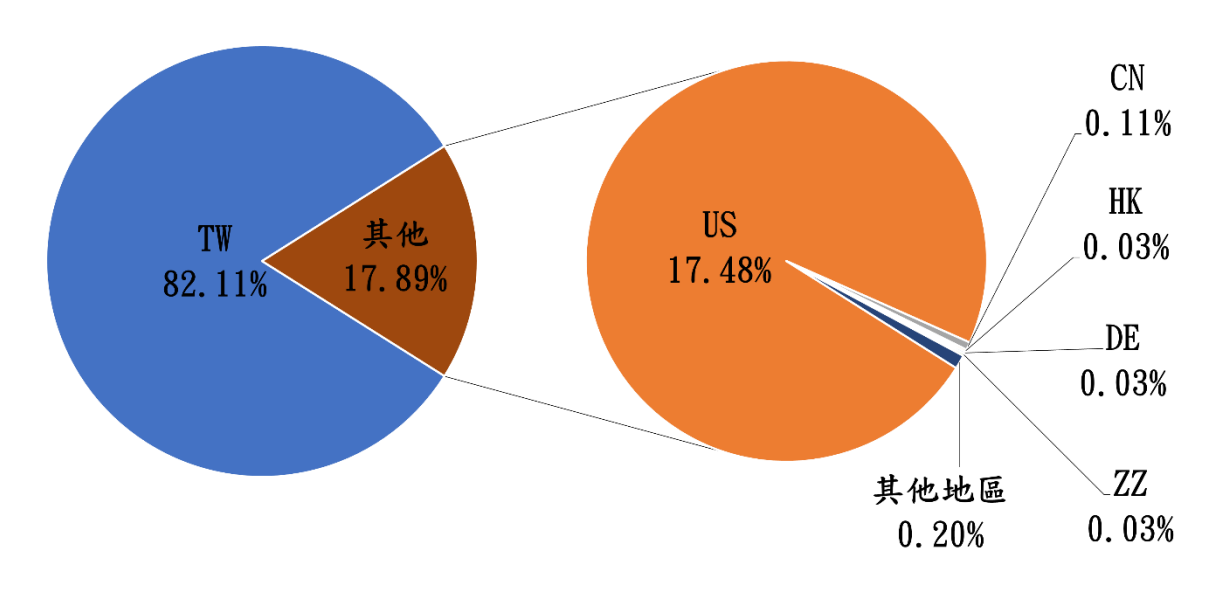


圖 1、分享地區統計圖

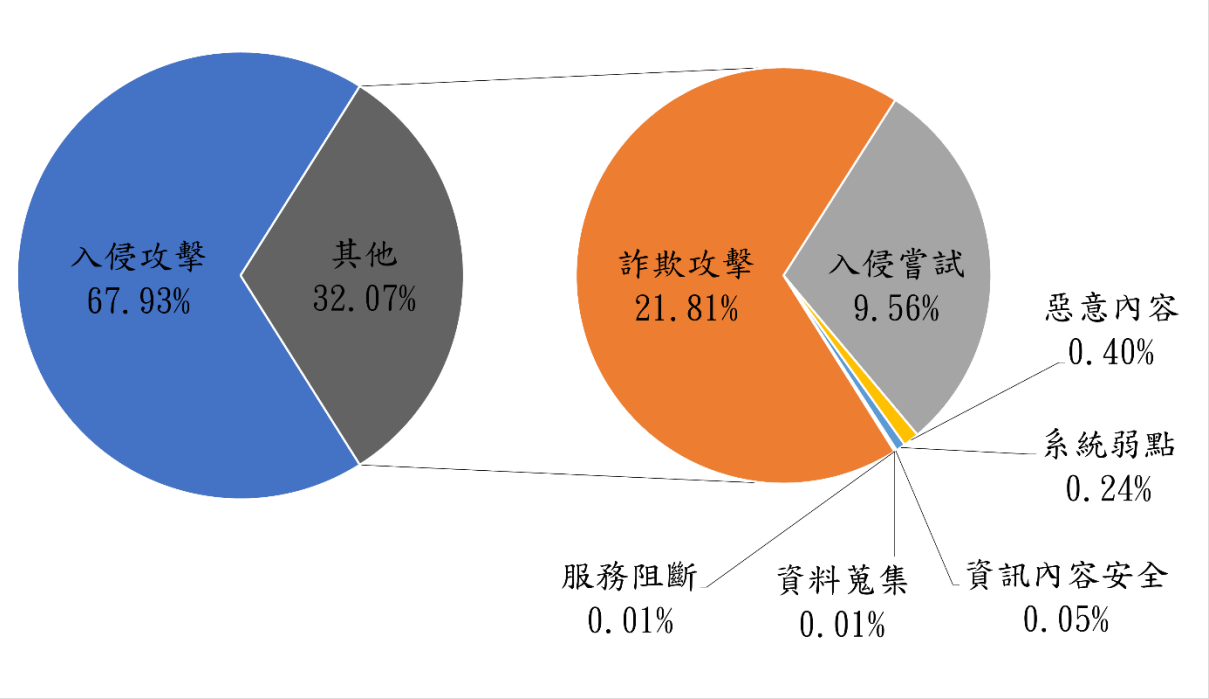

入侵攻擊
67.93%
其他
32.07%
詐欺攻擊
21.81%
入侵嘗試
9.56%
惡意內容
0.40%
系統弱點
0.24%
服務阻斷
0.01%
資料蒐集
0.01%
資訊內容安全
0.05%

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 8 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**