TWCERT/CC 資安情資電子報

2021 年 4 月份

目錄

第 1 章、 封面故事

美國資安單位針對微軟 Exchange 嚴重漏洞發布緊急修補命令

美國主管資安事務單位，日前針對微軟 Exchange 的多個嚴重 0-day 漏洞發布緊急修補命令，要求聯邦政府所屬單位，立即針對在其組織內運作的微軟 Exchange 系統進行資安修補。

美國主管資安事務的網路安全暨基礎設施安全局（Cybersecurity & Infrastructure Security Agency, CISA），日前針對 Microsoft Exchange 近期修補完成的四個嚴重 0-day 漏洞發布緊急修補命令。

CISA 發布編號為 Emergency Directive 21-02 的緊急命令，要求聯邦政府所屬單位，立即針對在其組織內運作的 Microsoft Exchange 系統進行資安修補。先前 CISA 也曾針對這四個漏洞發布資安通報，表示這些 0-day 漏洞已遭駭侵者大規模濫用。

在 CISA 發布的通報中指出，一共有四個 0-day 漏洞已獲得 Microsoft 修補完成並發表修補程式，分別是：

1、CVE-2021-26855：存於 Exchange Control Panel，駭侵者可透過特製的伺服器端連線要求，取得電子郵件與機密檔案的內容。

2、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065：這三個 0-day 漏洞皆可讓駭侵者遠端執行任意程式碼。

這些漏洞是由第三方資安廠商 Volexity 發現的。Volexity 除了詳細提出駭侵者可能採用的攻擊手法外，也觀察到駭侵者已透過某些 IP 發動攻擊。

CISA 的命令要求美國聯邦政府各單位，如有能力，應針對單位內部使用的 Exchange Server 進行徹底檢查，並依命令中的指示安裝更新軟體；如果單位沒有能力自行檢查並更新系統，應立即將所有 Microsoft Exchange Server 自外部網路離線，並依指示向 CISA 提出報告。

- CVE 編號：CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065
- 影響產品/版本：Microsoft Exchange Server 2010, 2013, 2016, 2019
- 解決方案：

  1、依 CISA Emergency Directive 21-02 指示徹底檢查系統。

  2、安裝微軟提供的各版本 Exchange Server 更新軟體。

- 資料來源：

  1. Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
  2. Mitigate Microsoft Exchange Server Vulnerabilities
  3. Released: March 2021 Exchange Server Security Updates
  4. Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabili

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、資安廠商指出，釣魚攻擊者發展出多種手法，使二階段驗證保護失去效力

資安廠商發表研究報告指出，駭侵團體已發展出多種手法，可以對應二階段驗證，使其失去保護能力。

資安廠商 SlashNext 日前發表研究報告指出，駭侵團體已發展出多種不同的手法，可以對應二階段驗證（Two-Factor Authentication, 2FA），使其失去原有的保護能力。

報告指出，二階段驗證過去一直被視為個人或企業保護登入過程的有力武器，可以有效阻隔各種意圖取得登入資訊的駭侵攻擊行動；然而所有的防護手法不可能是萬靈丹，駭侵團體已經發展出多種可使二階段驗證保護失去效力的手法：

1、中間人攻擊（Man-in-the-Middle Attacks）：許多公司行號允許員工在工作用電腦的瀏覽器中安裝多種外掛程式和擴充套件，藉以提升生產力。這類外掛程式和擴充套件雖然方便好用，但也潛藏資安風險，因為有些外掛程式和擴充套件內藏惡意程式碼，可以直接從瀏覽器畫面中取得所需資訊。

SlashNext 在報告中指出，該公司發現不少在外掛程式和擴充套件中暗藏惡意軟體的案例；這類惡意軟體只要坐等受害者完成二階段驗證流程，進入企業或網銀等重要系統網站後，再開始透過惡意程式碼，進行畫面截圖或資料竊取，再傳送給外部的惡意軟體控制伺服器，即可令二階段驗證的安全關卡完全失效。

2、詐騙技術支援（Techncal Support Scams）：在這類攻擊中，駭侵者會假扮成技術支援提供者，要求受害者安裝 TeamViewer 或 LogMeIn 之類的遙控登入軟體，接著就可以在受害者電腦中暗中植入各式惡意軟體，甚至感染整個內部網路。

3、二階段驗證詐騙視窗：駭侵者可藉由幾可亂真的詐騙二階段驗證視窗，取得受害者輸入的二階段驗證碼和用戶的登入資訊，甚至可藉由登入失敗畫面，向用戶騙取更多登入身份驗證所需的機敏資訊。

- 資料來源：
  1. Phishing Attacks that Defeat 2FA Every Time
  2. The State of Phishing 2021

2.1.2、2020 年資安調查：勒贖攻擊與釣魚攻擊大幅增加

資安廠商發表 2020 年針對 Windows 系統的全球惡意軟體駭侵攻擊統計結果，指出在去年一整年期間，一共偵測到高達 1.11 億起的感染事件。

資安廠商 Malwarebytes 與 VPN 服務商 Atlas VPN，日前聯合發表一分研究報告；報告中主要分析 2020 年針對 Windows 系統的全球惡意軟體（Malware）駭侵攻擊統計結果，並指出在去年一整年期間，Malwarebytes 一共偵測到高達 1.11 億起的感染事件。

報告中說，在各種作業系統中，Windows 是最常受到惡意軟體植入攻擊的對象，所以這份報告也以 Windows 系統的資料為主。

報告指出，在 2020 年一整年中偵測到的 Windows 惡意軟體植入攻擊中，有高達 9230 萬次攻擊，是針對消費者等級的 Windows 裝置發動攻擊，佔整體 1.11 億次攻擊事件的佔比高達 83%；而針對企業用 Windows 裝置的惡意軟體植入攻擊有 1670 萬次，佔總體約 15%。其餘 2% 的攻擊目標不明。

但值得注意的是，儘管 2020 年針對 Windows 的惡意軟體植入攻擊發生總次數高達 1.11 億次，但和 2019 相比，這個數字卻是下降的；2019 年同類攻擊的總次數高達 1.25 億次，2020 年比 2019 年下降了多達 12%。

針對消費性 Windows 的裝置，同類攻擊數量下降了 11%，而針對企業用 Windows 裝置的同類攻擊，降幅更高達 24%。

報告也分析了各種不同惡意軟體攻擊的次數與佔比。以 2020 年的統計來看，廣告軟體的攻擊次數最多，將近 3600 萬次，接下來依序是特洛伊木馬（近 3000 萬次）、駭侵工具軟體（近 1845 萬次）、高資安風險軟體（Riskware）（近 1411 萬次）、間諜軟體（288 萬次）等。

- 資料來源：
  1. Over 100 million malware infections detected on Windows in 2020
  2. Over 100 Million Malware Infections Detected On Windows In 2020 Says Atlas VPN

2.2、新興應用資安

2.2.1、QNAP NAS 已知漏洞遭駭侵者用以惡意挖礦

資安廠商近期發現有駭侵者利用 QNAP NAS 設備的兩個已知嚴重漏洞，大規模進行惡意挖礦攻擊。QNAP 各型 NAS 用戶應立即升級作業系統與受影響的應用程式，以避免遭到類似攻擊。

資安廠商 360 網絡安全研究院近期發表研究報告，指出該公司的未知威脅檢測系統，於 2021 年 3 月 2 日 發現駭侵者利用 QNAP 網路儲存系統（Network Storage System, NAS）設備的兩個已知嚴重漏洞，大規模進行惡意挖礦攻擊。

360 網絡安全研究院將這次攻擊命名為 UnityMiner，攻擊的主要手法是利用 QNAP NAS 的兩個已知嚴重等級安全漏洞 CVE-2020-2506 和 CVE-2020-2507，植入 XMRig 挖礦惡意軟體，利用 NAS 系統資源挖掘門羅幣（Monero）。

據 QNAP 官方於去年（2020 年）10 月發表的資安通報中，指出這兩個漏洞係存於 QTS 作業系統中的 Helpdesk 應用程式。CVE-2020-2506 為權限控制的錯誤，可讓攻擊者取得 QNAP NAS 裝置的控制權限，而 CVE-2020-2507 則是指令注入漏洞，可讓駭侵者遠端執行任意程式碼；這兩個漏洞都在當時推出的新版 Helpdesk 3.0.3 中修補完成。

360 網絡安全研究院在研究報告中指出，這波 UnityMiner 攻擊中，駭侵者利用了 QNAP NAS 的設備特性，將挖礦惡意軟體的執行緒，以及其真實的 CPU 與 RAM 使用資源的資訊隱藏起來，使得用戶無法從 QNAP 系統管理工具中看到該惡意軟體正在運作，因而難以發現系統的異常運作。

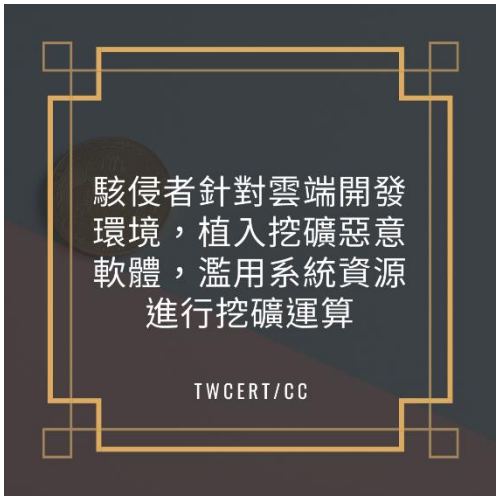
研究報告並未指明是哪個駭侵團體發動本次攻擊事件，但根據觀測報告，受影響的 QNAP NAS IP 共有高達 95 萬個，受害者數量最多的國家，依序為美國、中國、義大利、法國、德國、日本、英國、澳洲。

在該研究報告中也列出了所有受到影響的多款 QNAP NAS 型號，受影響機種多達 102 種；這批型號的韌體更新日期若在 2020 年 8 月之前，就都存有遭駭侵者此這兩個漏洞發動攻擊的風險。QNAP 各型 NAS 用戶應立即升級作業系統與受影響的應用程式，以避免遭到類似攻擊。

2020 年 10 月 7 日，QNAP 官方已發佈安全公告 QSA-20-08[1]，並指出已在 Helpdesk 3.0.3 和更高版本中解決了這些問題。

- 資料來源：
  1. QNAP NAS 在野漏洞攻擊事件 2
  2. Multiple Vulnerabilities in Helpdesk

2.2.2、駭侵者針對雲端開發環境植入挖礦惡意軟體，濫用系統資源進行挖礦運算



資安廠商發現針對雲端開發環境植入挖礦惡意軟體的攻擊事件，在沉寂數月後，近來又大舉發動攻擊。

資安廠商 Aqua 近日發表研究報告，指出該公司發現有駭侵者針對雲端開發環境植入挖礦惡意軟體的攻擊事件；這類駭侵攻擊活動在沉寂數月後，近來又開始大舉發動攻擊。

Aqua 指出，該公司旗下的「鸚鵡螺」（Nautilus）資安團隊，最早是在去年（2020）九月間發現這類攻擊事件。駭侵者針對在 Github 與 Docker Hub 上的自動化開發環境建置系統發動攻擊，在其開發環境中植入挖礦惡意軟體挖掘門羅幣。

Aqua 指出，去年該公司首次發現這類攻擊活動後，立即通知受到惡意攻擊的開發單位，相關的攻擊活動受阻後便沈寂了一段時間；近來該公司再度觀察到類似攻擊活動再度開始活躍，短短數日內就建置了 92 個 Docker Hub 註冊與 92 個 Bitbucket 程式庫，利用這些資源進行惡意挖礦活動。

Aqua 在報告中詳述了駭侵者採用的攻擊手法。首先駭侵者會利用位於俄羅斯境內的免費電子郵件服務 inbox.ru 設立多個攻擊用的 Email 帳號，接下來就利用這些 Email 帳號在 Bitbucket 網站內新增開發用的帳號與環境，並且利用一些技巧，將開發計畫偽裝為使用官方計畫文件設立的正常開發帳號，以避免被查緝。

駭侵者接著同時會申請新的 Docker Hub 帳號，同樣的，也會偽裝成使用官方計畫文件設立的開發者帳號來避開查緝，然後就開始執行多個偽裝成 ffmpeg、gcc 等通用程式，但實際上利用系統資源進行挖礦作業。

Aqua 指出，類似這類竊取雲端服務運算資源，實際上進行惡意挖礦攻擊的案例層出不窮。在 2020 年時 Bitbucket 也曾發生類似的駭侵挖礦攻擊。由於這類雲端開發環境服務，一般對於各專案的資安防護比較弱，也給駭侵者可乘之機。

- 資料來源：
  1. Threat Alert: Monero Miners Target Cloud Native Dev Environments
  2. Monero Mining Malware Secretly Installed On Bitbucket By Scammers

2.3、國際政府組織資安資訊

2.3.1、挪威國會受微軟 Exchange 漏洞影響遭駭

挪威國會的電腦系統遭到駭侵者利用微軟 Exchange Server 日前新發現的 ProxyLogon 漏洞攻擊，部分資料疑遭竊取。

挪威國會的電腦系統，日前遭到駭侵者利用微軟 Exchange Server 日前新發現的 ProxyLogon 漏洞攻擊，部分資料疑遭竊取。

挪威國會發表的資安通報指出，目前雖已針對此次駭侵攻擊事件展開調查，但目前尚無法確認受損範圍與損失程度，僅能確認有部分資料已遭駭侵者竊取；目前挪威國會已經會同該國司法機關與資安單位積極調查本次事件。

駭侵者用以攻擊挪威國會的 Microsoft Exchange Server ProxyLogon 漏洞，就是微軟在（2021 年）3 月 2 日緊急推出修補更新的四個嚴重漏洞，包括存於 Exchange Control Panel，可讓駭侵者透過特製的伺服器端連線要求，取得電子郵件與機密檔案內容的 CVE-2021-26855、可讓駭侵者遠端執行任意程式碼的 CVE-2021-26857、CVE-2021-26858、CVE-2021-27065 三個漏洞。

針對這四個嚴重漏洞，美國網路安全暨基礎設施安全局（Cybersecurity & Infrastructure Security Agency, CISA）曾在當時發布緊急修補命令，要求

美國政府各單位儘速安裝 Microsoft 推出的修補程式；微軟也在隨後發布資安通報，指出可能已有駭侵團體 Hafnium 利用這批漏洞，針對美國公私單位發動駭侵攻擊。

不過，以挪威國會的駭侵攻擊事件來說，目前沒有直接證據指出 Hafnium 與攻擊事件的關連性；資安廠商 ESET 也指出，除了 Hafnium 之外，該公司也觀察到其他駭侵團體如 Tick、LuckyMouse 和 Calypso 等，也在 Microsoft 發表修補程式之前，就開始利用 ProxyLogon 漏洞發動駭侵攻擊。

- 資料來源：
  1. Norway parliament data stolen in Microsoft Exchange attack
  2. New nation-state cyberattacks
  3. Norwegian government falls victim to Microsoft attacks

2.3.2、波蘭政府網站遭駭，用以散布不實輻射污染訊息

兩個波蘭政府擁有的網站，於日前遭到駭侵攻擊，用以散布不實的輻射污染訊息。

兩個由波蘭政府擁有的網站，於 2021 年 3 月 17 日遭到來源不明的駭侵攻擊，駭侵者利用這兩個網站散布不實的輻射污染訊息，企圖製造恐慌與混亂。

據波蘭警方表示，波蘭國家原子能管理署和衛生部的官方網站，被駭侵者駭入後，於網站上張貼不實的核子污染物外洩假消息，假消息內容指波蘭鄰國立陶宛發生幅射外洩事件，波及波蘭境內。

不只是兩個政府網站遭駭侵者用以散布這類輻射污染不實訊息，一個經常撰寫俄羅斯與東歐各國事務的記者，其 Twitter 帳號也同時遭駭，同樣用來散布相同的假訊息。

這波假訊息要求波蘭境內居住在鄰近立陶宛邊境「災區」的人員，要提高警覺，注意自己是否遭到輻射污染；所幸這則不實訊息並未引起民眾的過度反應。

波蘭資安最高官員 Stanislaw Zaryn 在接受媒體採訪時指出，這是典型的不實訊息攻擊案例，意圖升高波蘭與其他西方盟國之間的歧見，是一種分化的手段。

Zaryn 指出，2020 年時發生過類似的假訊息認知攻擊，當時駭侵者散布的不實訊息內容，是指發生於 1980 年代發生在今烏克蘭境內的車諾比爾核能電廠爐心熔毀事件，當時的輻射物質飄散到波蘭境內，但這並非事實。

- 資料來源：
  1. Polish state websites hacked and used to spread false info
  2. Polish state websites hacked, spreading false report of radioactive threat
  3. Polish State Websites Hacked and Used to Spread False Info

2.4、社群媒體資安近況

2.4.1、日本 LINE 不慎讓其中國關係企業人員存取用戶個資與對話內容

通訊軟體 LINE 日本公司發生個資控管失當事件，其中國關係企業的開發人員，自 2018 年以來多次存取 LINE 日本用戶多項個資和對話內容。

在日本、台灣與東南亞各國擁有大量用戶的通訊軟體 LINE，其日本公司發生個資控管失當事件。該公司的母公司在中國設立的子公司開發人員，自 2018 年以來多次在未經用戶同意的情形下，不當存取 LINE 日本用戶多項個資與對話內容。

據日本媒體報導，LINE 在關係企業開發廠商旗下的開發人員，自 2018 年起在未經用戶同意的情形下，不當進入日本 LINE 伺服器存取日本 LINE 用戶各項資訊的次數，達到 32 次以上。

據報導指出，被不當存取的日本 LINE 用戶個資，至少包括使用者姓名、Email 地址與手機電話號碼，甚至包括對話內容等。

報導指出，LINE 是透過母公司 Z Holdings（ZHD）委託位於上海的關係企業技術開發公司，共同研發用於多項新業務的人工智慧技術；可以接觸到日本 LINE 用戶的開發者共有 4 名。

日本 LINE 公司在二月發現這件資安事件後，除了取消中國開發人員的資料存取權限外，也已在日前向日本政府的個人情報保護委員會提出報告，並且會同第三方單位成立調查委員會，對整起事件進行調查，並做出改善命令。

LINE 指出，目前的調查結果並未顯示個資遭到不當濫用；在 LINE 日本的個人情報保護說明中雖然提到，用戶的個資可能會移轉到第三國進行處理，但並未說明會移轉到哪個國家。

此外，日本的個人情報保護法（相當於台灣的個人資料保護法）中，雖然規定日本企業若將用戶個人資料移轉給日本國內業者處理時，無需經過用戶同意，但若移轉到外國廠商時，則需取得用戶同意。

日本個人情報保護委會員指出，目前正在修訂中的新版個人情報保護法，將增列個人情報轉移至海外處理時，必須載明轉移目的國名稱的條款；新版法案預定於 2022 年 6 月開始生效。

- 資料來源：
  1. 「ＬＩＮＥ」個人情報が丸見え、管理委託の中国企業から…運用見直しを検討
  2. LINE の個人情報、中国から閲覧できる状態　2018 年 8 月から
  3. Line silently exposed Japan user data to China affiliate

2.4.2、LINE 日本用戶個資外洩事件，致使諸多公私單位暫停使用

日前 LINE 發生中國關聯會社開發者任意存取日本用戶個資事件後，已有眾多日本各級政府單位與私營企業，宣布暫停使用 LINE。

免費通訊軟體 LINE，日前發生其母公司所屬的中國關聯會社開發者任意存取日本用戶個資事件後，在日本社會引發高度衝擊；至今已有眾多日本各級政府單位與私營企業，宣布暫停使用 LINE。

事件發生後，日本 LINE 公司除了配合行政當局和第三方機構展開調查外，也完全禁止來自中國的網路存取；但該公司也被發現將用戶上傳的圖片和影片等多種資料儲存於南韓境內的伺服器，風暴因而愈演愈烈。

日本 LINE 公司於 2021 年 3 月 23 日針對資料外洩與境外儲存問題，召開記者會加以說明；該公司指出，除了日本之外，包括台灣和其他市場用戶上傳的圖片和影像等資料，確實都儲存在位於韓國境內的伺服器。

LINE 也指出，不只是影像資料，包括在日本推出的診斷服務「LINE DOCTOR」，也將相關的資料，例如醫療保險證、收據、診斷明細、醫師確認過的相關文件，甚至合作醫師的相關證照資料等，也存放在韓國伺服器中。

LINE 說，這些資料在儲存時都經加密，也非永久存放，不過並未具體說明存放期限；LINE 也說由於其韓國母公司有許多資料中心的人才和完善的基

礎建設，從成本考量上，將資料存放在韓國伺服器是很合理的。

不過 LINE 在記者會中也承諾，今後會逐步將存在韓國伺服器中的資料，移回日本境內的伺服器，社長也在記者會上致歉。

由於 LINE 日本公司的個資保護問題，許多日本原本使用 LINE 與用戶溝通的公私單位，近期紛紛表示將暫停使用；宣布停用的日本各級政府包括內閣官房長官、總務省、厚生勞動省、京都府、大阪市、廣島市、岐阜縣、千葉縣、鳥取縣等，私營企業則包括日本趨勢科技、日本郵便、日本航空、全日空等。

- 資料來源：

1. LINE のデータ保管、なぜ海外に？　LINE 幹部が会見で説明
2. トレンドマイクロ、LINE を使ったサービスを停止
3. LINE・出澤社長が会見(全文 1)中国からの完全アクセス遮断

2.4.3、美國社群網站 Gab 遭駭，多種用戶機敏資訊被竊

美國另類右翼人士聚集的社群網站 Gab 日前遭到駭侵者攻擊，造成多種用戶資料被竊走，包括用戶密碼與通訊內容。

在美國選戰末期開始湧入大批另類右翼用戶的美國社群網站 Gab，日前遭到一個不明駭侵者的攻擊，導致高達 70GB 的站內資料被竊；攻擊者並將這批資料轉交給一個稱為「分散式機密阻斷」（Distributed Denial of Secrets），該組織是個類似 WikiLeaks 的吹哨者非營利民間團體。

據資訊媒體 Wired 的報導指出，在這 70GB 的資料中，至少包括四千萬篇用戶貼文，其中包括在 Gab 上的各種公開貼文和用戶描述檔案（但不包括上傳到 Gab 的相片和影片），也包括私人討論群組內的內容、個人帳戶的私密貼文與所有通訊內容，甚至也包括用戶在 Gab 上使用的登入密碼在內。

Wired 指出，在另一個以完全沒有言論審查機制的社群網站 Parler，因其上的各種過激與仇恨言論，遭到 Google、Apple、Amazon 等封鎖，導致 Parler 無法正常運作後，原本在 Parler 上的各種右派用戶，便大舉轉移使用原本就是偏右立場的 Gab。

Distributed Denial of Secrets 的共同創辦人 Emma Best 在 Wired 的訪問中說，由於從 Gab 取得的資料太過敏感，因此 Distributed Denial of Secrets 將不會直接公開這批資料；Distributed Denial of Secrets 將會選擇性地釋出部分資料給予媒體記者、社會學家、相關研究者，以了解這些用戶的

組成、言論內容和行為。

Gab CEO Andrew Torba 則在其他的專訪中承認，該公司確實遭到駭侵攻擊，導致資料被竊；該公司針對此次駭侵事件，於官方部落格中發表了一篇資安通報，指出用戶密碼經過加密儲存，但私人群組的密碼則未經加密。

- 資料來源：
  1. Alleged Data Breach – 26 February 2021
  2. GabLeaks
  3. Far-Right Platform Gab Has Been Hacked—Including Private Data

2.5、行動裝置資安訊息

2.5.1、假冒 Android 版 Clubhouse app，大量竊取用戶手機儲存的登入資訊

資安專家近期發現一個假冒為 Android 版 Clubhouse 的惡意行動應用程式，會竊取用戶手機內儲存的 458 種網路服務的登入資訊。

資安廠商 ESET 旗下的資安專家近期發表研究報告，指出該單位發現一個假冒為 Android 版 Clubhouse 的惡意行動應用程式；這支假 app 會竊取用戶手機內儲存的 458 種網路服務的登入資訊。

報告指出，這個惡意 Android app 假冒目前廣受歡迎，仍為邀請制，且僅推出 iOS 版本行動應用程式的 Clubhouse，將 Clubhouse 官網上的資訊和外觀包裝在 app 中，但內含一個稱為「BlackRock」的特洛依木馬惡意程式。

用戶一旦受騙安裝了這個假冒的 Android app，不但無法如 iOS 版官方 app 一樣進行社群聊天，還會被 BlackRock 在手機中搜刮多達 458 種不同網路服務的登入帳號與密碼；會被竊取登入資訊的服務包括 Twitter、Facebook、WhatsApp、Amazon、Netflix、Outlook、eBay、Coinbase、Plus500、Cash App、BBVA、Lloyds Bank 等。

資安專家指出，一般正常的官方網站，如果讓用戶下載行動應用程式，通常都會導向到 Google Play 或 Apple App Store 等官方應用程式商店，但

像這次假冒 Clubhouse Android 版 app 的案例，用戶在按下「Get it on Google Play」按鈕後，並不會被導向到 Google Play 商店，而是會直接下載 apk 應用程式安裝套件。

用戶一旦發現自己沒有被導向到官方應用程式商店，而是直接下載安裝套件，就應立即提高警覺，不要安裝該套件。

- 資料來源：
  1. Beware Android trojan posing as Clubhouse app
  2. Bogus Android Clubhouse App Drops Credential-Swiping Malware
  3. Fraudsters jump on Clubhouse hype to push malicious Android app

2.5.2、Samsung 推出 2021 年三月份更新包，修復多個 Android 嚴重資安漏洞

韓國行動裝置大廠 Samsung 近日推出 2021 年三月份更新包，修復多個存於 Android 行動作業系統中的資安漏洞，Samsung 行動裝置用戶應立即更新裝置。

韓國行動裝置大廠 Samsung 近日推出 2021 年三月份更新包，修復多個存於 Android 行動作業系統中的資安漏洞，其中包括一個嚴重漏洞及多個高危險漏洞；Samsung 行動裝置用戶應立即更新裝置。

這些獲得更新的漏洞散見於執行階段、作業系統等相關組件中，總數共有 11 個；Samsung 是在 Google 推出 2021 年三月份的 Android 作業系統更新後，緊接著推出該品牌部分行動裝置適用的資安更新升級包。

據資安媒體 BleepingComputer 指出，該刊發現部分 Samsung Galaxy 系列裝置在 3 月 5 日開始陸續進行自動更新。

這次的更新中修復的最嚴重資料漏洞，首推編號為 CVE-2021-0397 的嚴重等級漏洞。這個漏洞存於 Android 作業系統中的藍牙連線裝置搜尋功能；駭侵者可以透過特製的藍牙資料傳輸觸發一個空指標（null pointer）錯誤，遠端執行任意程式碼。

其他在這次得到修復的的資安漏洞如下：

- CVE-2021-0395：系統重新啟動時的使用已釋放記憶體錯誤，可導致駭侵者提升執行權限；

- CVE-2017-14491：資料堆積記憶體暫存溢位錯誤，可導致駭侵者遠端執行任意程式碼；
- CVE-2021-0393：LiteralBuffer 錯誤，可導致駭侵者遠端執行任意程式碼；
- CVE-2021-0396：參數計數的差一錯誤（off-by-one），可導致駭侵者遠端執行任意程式碼。

Samsung 這次推出的資安漏洞修補包，除了修補上述資安漏洞外，也針對該公司自行開發的多個行動應用程式加強其功能；Samsung Galaxy 系列行動裝置（手機、平板）的用戶，均應立即更新系統，以避免駭侵者利用上述漏洞發動攻擊。

- 資料來源：
  1. Galaxy S10 5G (SM-G977B)
  2. Android 安全公告-2021 年 3 月
  3. Samsung fixes critical Android bugs in March 2021 updates

2.5.3、204 個 iOS、Android 行動「騙錢軟體」，詐騙金額高達 4 億美元

資安專家指出，在 Google Play 和 Apple App Store 中，存有數百個「騙錢軟體」，累積的詐騙不法所得高達 4 億美元。

資安廠商 Avast 旗下的資安專家，近日發表研究報告指出，在 Android 的 Google Play 和 iOS 的 Apple App Store 中，存有高達 204 種不同的「騙錢軟體」（fleeceware），累積的詐騙不法所得高達 4 億美元。

所謂的 fleeceware 騙錢軟體，是指一種會在用戶不知情的情況下，暗中向用戶收取高額費用的惡意軟體；這類 fleeceware 通常會以免費軟體的形態，誘使用戶下載安裝在自己的手機上，然後利用多數用戶不清楚 Google Play 和 App Store 扣款機制的弱點，誘使用戶同意在試用期結束後開始扣款。

這類騙錢惡意軟體的免費試用期限通常很短，有些僅有三天，用戶接下來就必須支付極高的定期扣款費用，典型的案例每周會向用戶收取 4 到 12 美元的費用，一年相當於 208 美元到 624 美元；部分案例甚至每周向用戶收取 66 美元，一年下來高達 3,432 美金。

另外，除非用戶到 Google Play 或 App Store 中進行退訂手續，不然即使用戶在手機上移除了這類騙錢軟體，仍然會繼續遭到扣款。

據 Avast 的研究報告說，該團隊找到的這類 fleeceware，種類包括多種熱門應用類型，像是樂器演奏相關的 App、電子書閱讀器、相片編輯美化工具、拍照濾鏡、星座算命、QR Code 掃瞄器、PDF 閱讀器等等。通常這些騙錢軟體都會實作出標榜的功能，但卻會隱藏高額扣款的相關資訊。

這些惡意騙錢軟體往往也會透過洗評價的方式，利用人頭帳號在 App Store 和 Google Play 的軟體評價留言中大量製造虛假的正面評價，以吸引用戶上鉤。用戶在下載任何 App 時均需提高警覺，詳加注意付費周期與額度資訊，收費若不合理即應避免下載。

- 資料來源：
  1. How fleeceware apps have earned over $400 million on Android and iOS
  2. Hundreds of fleeceware apps earn dubious iOS, Android developers over $400 million

2.5.4、新發現 XcodeSpy 開發環境惡意軟體，意圖對 iOS 開發者發動供應鏈攻擊

資安專家近期發現一個惡意的 Xcode 開發計畫案，專門針對 iOS 軟體開發者下手，可在開發者的電腦中安裝後門，發動供應鏈攻擊。

資安廠商 SentineOne 旗下的資安研究人員，近期發現命名為「XcodeSpy」的一個惡意 Xcode 開發計畫案；這個計畫案專門針對 iOS 軟體開發者下手，可在開發者用以撰寫 iOS 應用程式的 Mac 電腦中安裝後門，發動供應鏈攻擊。

研究人員發現某個沒有問題且常被使用的 Xcode 開發計畫「TabBarInteraction」，有部分版本被植入了 XcodeSpy 惡意程式碼；駭侵者在 TabBarInteraction 正常的程式碼之外，另外加入了用以執行惡意攻擊的一段 Run Script 程式碼。

當程式開發人員建置含有 Run Script 的開發計畫案時，Xcode 會自動執行 Run Script，並且在開發人員用的電腦上開啟一個可遠端控制的後門，並且連上駭侵者布置的控置伺服器，其網址為 cralev.me。

研究人員指出，這段指令碼會在 /tmp 目錄中製作一個檔名為 .tag 的隱藏檔，其中包含了 :mdbcmd 指令，以便連上駭侵者布置的控制伺服器，發動各種後續攻擊。

不過 SentineOne 也表示，當他們發現 XcodeSpy 的存在時，程式碼指向的控制伺服器已經無法連線，因此目前不知道駭侵者會透過這個後門，發動何種類型的攻擊活動。

據研究人員指出，XcodeSpy 開啟的後門稱為 EggShell 後門，可以讓駭侵者上傳或下載檔案、遠端執行各種指令，同時竊取用戶透過鍵盤、麥克風與攝影鏡頭的活動資訊。

- 資料來源：
  1. New macOS malware XcodeSpy Targets Xcode Developers with EggShell Backdoor
  2. New XcodeSpy malware targets iOS devs in supply-chain attack
  3. New XcodeSpy Mac Malware Targets Software Developers

2.6、軟體系統資安議題

2.6.1、QNAP 警示 NAS 用戶提防暴力試誤攻擊

台灣網路儲存設備大廠 QNAP 日前發出資安警示，指出觀察到大量針對其裝置的暴力登入試誤攻擊；用戶應提高警覺，並進行必要的安全設定。

台灣網路儲存設備（Network Storage System, NAS）大廠 QNAP 日前發出資安警示，指出該公司目前觀察到大量針對其裝置的暴力登入試誤攻擊；用戶應立即提高警覺，並進行必要的安全設定，提升防護能力，以避免裝置遭到駭入造成損失。

QNAP 發出的資安警示指出，該公司近來接到多名用戶反應，指出其裝置遭到不明駭侵者發動的暴力登入試誤攻擊。QNAP 說，如果用戶在自己的 NAS 上使用預設帳號密碼，或是帳號密碼設定為像是「password」、「12345」之類容易被猜中的密碼，就很容易被這類攻擊順利駭入。

QNAP 建議所有其品牌 NAS 裝置用戶，不分機型、不論韌體版本為何，均應立即採取以下行動，提升 NAS 裝置的資安防護能力：

- 勿將 NAS 系統曝露在外部網路可存取的範圍內，應以防火牆加以隔絕，僅開放絕對必要的對外連接埠；
- 一些常用的網路服務類型，如 http、https、FTP、sFTP、Telnet、SSH、SMTP、POP3、IMAP、SAMBA、AFP 等連接埠，應避免使用預設值，最好改用自定埠號；

- 使用更長、安全層級更高的登入密碼；
- 可將預設且無法刪除的登入帳號如 admin 等自系統上停用 (disable)，改用自訂的管理員帳號，提高暴力登入試誤的難度；
- 如果無法更改常用通訊協定（http、https、FTP、sFTP、Telnet、SSH、SMTP、POP3、IMAP、SAMBA、AFP）等的連接埠埠號，則應在控制面板的「System」-「Security」-「IP Access Portection」中設定阻擋規則，同一個 IP 在一分鐘以內超過 5 次連線失敗的話，就將之列入永久拒絕連線的黑名單中。
- 檢查是否有不明的裝置使用者帳號，將之全部移除，以免遭到破解而入侵系統。
- 定期備份 NAS 內的重要資料。

- 資料來源：
  1. Take Action to Protect Your QNAP Devices From Brute-Force Attacks
  2. What to do if there are constant unauthorized attempts to access the NAS using the “admin” user, wit
  3. QNAP warns of ongoing brute-force attacks against NAS devices

2.6.2、雲端監視服務遭駭，車廠、醫院、監獄、公司行號影像被公開

一家提供企業級雲端影像監控業務的新創公司，其布署在多家客戶的錄影監視器畫面遭駭侵者取得並公開，受害者包括電動車廠 Tesla、雲端服務提供者 Cloudflare、監獄、以及多家銀行和醫院等。

一家名為 Verkada，提供企業級雲端影像監控業務的新創公司，其布署在多家客戶的錄影監視器畫面遭駭侵者取得並公開；受害者包括電動車廠 Tesla、雲端服務提供者 Cloudflare、監獄、以及多家健身房、銀行和學校、警局、醫院、診所等。

在駭侵者公開的畫面中，可以清楚看到 Tesla 與 Cloudflare 辦公室內的影像，此外被公開影像的 Verkada 用戶還包括幾家婦科診所、精神科門診、健身中心、銀行分行等等。

該駭侵團體其中一名負責逆向工程的成員，日前在 Twitter 上發表一系列該團體取得的監視器畫面；該團體宣稱握有可存取 Verkada 所有監視器畫面與影像資料庫的帳號密碼，同時在 Twitter 上貼出一張據稱是 Verdaka 管理系統以 Linux root 帳號登入的畫面，其中可以看到網路卡的 MAC adress，該 MAC address 即屬於 Verkada 研發的監控裝置網路界面所有。

該駭侵團體也宣稱，發動 Verkada 駭侵攻擊的目的，是要提醒世人更加關切監視系統無所不在，但極為脆弱，很容易遭到駭入的現實。

Verkada 在獲知該公司的系統遭駭侵攻擊後，便取消了駭侵者持有的帳號密碼與其存取權限 ；在 Verkada 發表的資安通報中，指出該公司的一台用於客服系統進行大量裝置維護管理的 Jenkins 伺服器，於 2021 年 3 月 7 日到 9 日間遭到不當存取，駭侵者取得的帳號與權限，有能力跳過該公司的各項安控機制，包括二階段驗證。

但該公司也在通報中強調，目前調查結果並未顯示用戶帳號密碼遭竊，Verkada 本身內部網路和財務等營運系統也未遭駭侵攻擊；至於可能被取得的資訊，則包括部分客戶的影像資料與客戶端系統管理人員的姓名、Email 地址、Verkada 本身的一些銷售資訊等。

- 資料來源：
  1. Latest Security Update
  2. Hackers access surveillance cameras at Tesla, Cloudflare, banks, more
  3. Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

2.6.3、美國大型啤酒廠疑遭勒贖駭侵攻擊，導致生產受阻

美國大型啤酒廠 Molson Coors 日前疑似遭到勒贖攻擊，導致啤酒生產流程中多個系統無法正常運作。

美國大型啤酒廠 Molson Coors 日前疑似遭到不明駭侵團體發動的勒贖攻擊，導致啤酒生產流程中多個系統無法正常運作，包括釀造、包裝和出貨等部門的工作都受到阻礙。

Molson Coors 是在 2021 年 3 月 11 日遭到駭侵攻擊，隨即向美國證管會（Securities and Exchange Commision, SEC）遞交 8K 重大訊息通報文件；文件中指出該公司「因為資安事件而發生系統故障」；該公司已經會同外部資安廠商進行事件調查，然而並未揭露調查所得的相關資訊。

雖然 Molson Coors 並未揭露該公司遭到哪一種類型的駭侵攻擊，但資安專家根據各種跡象研判，很可能是勒贖攻擊所致；資安廠商 Nozomi Networks 指出，攻擊這類大型企業的利潤十分豐厚，特別是像 Moslson Coors 這類全球啤酒廠之類的大型企業，最近經常成為勒贖攻擊的對象。

另一家資安廠商 Red Canary 則指出，勒贖攻擊造成的資料損失，對製造業者的傷害非常嚴重；一方面不只是無法存取過往的各種資料，在製造流程上累積的各種最佳化參數一但流失，將對整個製造和出貨的流程造成嚴重打擊，以致影響公司獲利能力。

近年來這類針對大型製造業發動攻擊，造成受害者生產受阻的案例愈來愈頻繁；三月初法國 Groupe Beneteau 造船廠遭到攻擊後，造成生產停頓數日之久，而在二月時包裝大廠 WestRock 也遭到駭侵攻擊，導致該公司的 IT 系統與生產管理系統無法運作。

Molson Coors 生產多種暢銷品牌啤酒與各式飲料，包括 Coors Light、Miller Lite、Molson Canadian、Carling、Coors Banquet、Blue Moon 等。

- 資料來源：
  1. UNITED STATES SECURITIES AND EXCHANGE COMMISSION MOLSON COORS BEVERAGE COMPANY
  2. Molson Coors Cracks Open a Cyberattack Investigation
  3. Cyberattack Forces Brewery Shutdown at Molson Coors

2.6.4、無線 IoT 設備製造商 Sierra Wireless 遭勒贖攻擊

全球無線 IoT 裝置製造大廠 Sierra Wireless，日前發表資安通報，指出該公司遭到不明來源的駭侵勒贖攻擊，導致所有生產基地和部分網路服務無法運作。

總部位於加拿大溫哥華的全球無線 IoT 裝置製造大廠 Sierra Wireless，於 2021 年 3 月 23 日發表資安通報，指出該公司在 2021 年 3 月 20 日遭到不明來源的駭侵勒贖攻擊，導致所有生產基地和內部網路無法運作。

在該公司發布的資安通報中說，該公司在遭到攻擊的第一時間，就針對受到攻擊的系統進行緊急處理，並且會同第三方資安專家共同調查事故起因，同時努力讓受駭系統恢復正常運作。

Sierra Wireless 說，目前災情造成所有生產基地的運作無法正常進行，該公司的官方網站和部分內部維運系統也受到影響；但內部 IT 系統和提供外部顧客使用的系統，則因為與其他系統隔開而未受波及。

Sierra Wireless 的資安通報中，沒有針對這次勒贖攻擊的細節提供任何資料；包括勒贖團體名稱、其使用的勒贖工具、哪些資料遭竊、要求的贖金高低，以及該公司是否支付贖款等情報，均沒有提供；該公司也沒有回應多家資安相關媒體的採訪詢問。

在 Sierra Wireless 提供的資安通報中指出，由於該起駭侵事件，該公司必須撤回在 2021 年 2 月 23 日依法發佈的 2021 年第一季業務展望報告。

近來大型製造業因勒贖攻擊因而造成生產停擺的案例時有所聞，包括美國啤酒製造大廠 Molson Coors 與包裝業龍頭廠商 WestRock，今年也都傳出因勒贖攻擊而造成生產線無法運作的消息。

- 資料來源：
  1. Sierra Wireless Announces Ransomware Attack
  2. Ransomware attack shuts down Sierra Wireless IoT maker
  3. Sierra Wireless Says Ransomware Disrupted Production at Manufacturing Facilities

2.7、軟硬體漏洞資訊

2.7.1、Google Chrome 修復嚴重 0-day 資安漏洞，請用戶立即更新

Google 於日前推出 Chrome 瀏覽器更新，修復多個資安漏洞，其中包括一個嚴重漏洞，可能導致駭侵者遠端執行任意程式碼，用戶應立即更新至最新版本。

Google 於日前推出 Chrome 瀏覽器更新版本 89.0.4389.72，修復多個資安漏洞，其中包括一個嚴重漏洞，可能導致駭侵者遠端執行任意程式碼，用戶應立即更新至最新版本。

這個編號為 CVE-2021-21166 的資安漏洞，存於 Chrome 處理音訊的子系統中；該段程式碼在處理音訊物件的生命周期時存有錯誤，駭侵者若將用戶導向到特製的網頁，即可觸發此錯誤，造成堆疊暫存區的溢位錯誤，藉以遠端執行任意程式碼。

這個漏洞的 CVSS v3 危險程度評分高達 8.8 分，危險程度分級達到嚴重（critical）等級。存有這個漏洞的 Google Chrome 為各主要作業系統（Windows, Mac, Linux）89.0.4389.71 之前的各個 Chrome 89 版本。

據 Google 發表的資安通報指出，該公司已掌握此一漏洞遭外界大規模濫用的情資；Google 已於資安通報發表的同時，推出新版 Chrome 89.0.4389.72 版本，修復此一嚴重漏洞；用戶應立即更新到最新版本，以避免遭駭侵者利用此漏洞發動攻擊。

除此漏洞之外，新推出的 Chrome 89.0.4389.72 版本，同時也修復了另外 46 個嚴重程度較低的資安漏洞，其中危險程度等級較高的漏洞包括：

1. CVE-2021-21159：TabStrip 組件中的 Heap 暫存記憶體溢位錯誤；
2. CVE-2021-21160：WebAudio 組件中的 Heap 暫存記憶體溢位錯誤；
3. CVE-2021-21161：TabStrip 組件中的 Heap 暫存記憶體溢位錯誤；
4. CVE-2021-21162：WebRTC 使用已釋放記憶體的錯誤；
5. CVE-2021-21163：閱讀模式中資料驗證不足；
6. CVE-2021-21164：iOS 版本資料驗證不足。

- CVE 編號：CVE-2021-21166
- 影響產品/版本：Google Chrome 89.0.4389.71 之前的各個 Chrome 89 Windows、Mac、Linux 版本
- 解決方案：升級至 Chrome 89.0.4389.72

- 資料來源：
  1. Stable Channel Update for Desktop
  2. #VU51166 Improper control of a resource through its lifetime
  3. New Chrome 0-day Bug Under Active Attacks – Update Your Browser ASAP!

2.7.2、iPhone 破解團體推出可適用於幾乎所有 iPhone 機種的新越獄軟體

iPhone 破解團體利用先前 Apple 發布過資安通報的漏洞，發展出全新的越獄工具，幾乎適用於所有機型的 iPhone。

一個 iPhone 破解團體日前利用先前 Apple 發布過資安通報的漏洞，發展出全新的越獄工具；該越獄工具幾乎適用於所有機型的 iPhone。

這個名為 The Unc0ver team 的 iPhone 破解團隊，在二月底釋出全新的 iPhone 越獄工具，可以幫助用戶繞過 iOS 系統的各種權限與安全設定，自行安裝未於 App Store 中上架的各類越獄機專用軟體，或是繞過系統的某些限制，執行 Apple 基於各種理由（例如資安、電力消耗、隱私保護、商業利益等）未曾開放的功能。

The Unc0ver team 表示，新的 iPhone 越獄工具可在 iOS 11 到 iOS 14.3 之間的所 iOS 版本上執行，支援的硬體幾乎涵蓋所有市面上仍可運作的各式 iPhone 手機或 iPad 平板。

The Unc0ver team 在其官方推文中指出，該團隊透過自行開發的駭入手法，利用 CVE-2021-1782 這個存於 iOS 作業系統核心中的漏洞，得以破解 iOS 的權限限制，讓用戶帳號取得系統等級的執行權限。

The Unc0ver team 這個最新越獄工具利用的 CVE-2021-1782 漏洞，曾經在 Apple 於二月初發表的資安通報中被列出；在該通報中 Apple 指出該公

司已掌握此漏洞已遭外界大規模濫用的情資。

CVE-2021-1782 這個漏洞，也已在 Apple 近期推出的 iOS 14.4 中修復，因此 The Unc0ver team 推出的越獄工具，在已更新至 iOS 14.4 的 iPhone 或 iPad OS 14.4 的 iPad 平板上是無法執行的。

長久以來資安專家不斷呼籲，任何 iPhone 和 iPad 用戶都不應任意在自己的裝置上使用越獄工具破解作業系統限制，更不應安裝未經官方 App Store 認可上架的第三方應用程式，因為這將會大大提高裝置遭到各種駭侵攻擊的風險；而為了防止其他惡意軟體透過已知的漏洞駭入用戶裝置，用戶也應在作業系統發布更新時立即套用更新，以確保裝置的安全性。

- CVE 編號：CVE-2021-1782
- 影響產品/版本：iOS、iPad OS 11 至 14.3，iPhone 6s 之後所有版本、iPad Air 2 之後所有版本、iPad mini 4 之後所有版本、iPod Touch 第 7 代
- 解決方案：更新至 iOS、iPad OS 14.4 之後版本

- 資料來源：
  1. @Pwn20wnd (TWITTER)
  2. About the security content of iOS 14.4 and iPadOS 14.4
  3. Hackers release a new jailbreak tool for almost every iPhone

2.7.3、Facebook 官方 WordPress 擴充套件修復兩個嚴重漏洞

資安廠商發現 Facebook 官方推出的 Facebook for WordPress 擴充套件，存有兩個可讓駭侵者遠端執行任意程式碼的嚴重漏洞，使用該套件的用戶應立即更新。

專攻 WordPress 資安領域的資安廠商 Wordfence，日前發表研究報告指出， Facebook 官方推出的 Facebook for WordPress 擴充套件，存有兩個可讓駭侵者遠端執行任意程式碼的嚴重漏洞；這兩個漏洞都已在新版 Facebook for WordPress 中修復，使用該擴充套件的用戶，應立即更新至最新版本。

Facebook for WordPress 是由 Facebook 官方推出的 WordPress 擴充套件，可讓 WordPress 架站管理者在其 WordPress 部落格中放置 Facebook Pixel 追蹤像素，用以追蹤訪客在網站上的使用足跡，除了可提供管理者更精確的網站統計報告外，也能讓 Facebook 藉以遞送精準廣告。據估計，超過 50 萬個 WordPress 網站，都安裝了 Facebook for WordPress 擴充套件。

據 Wordfence 的報告指出，這兩個漏洞，有一個是利用 POP Chain 植入 PHP 物件的漏洞，駭侵者可以利用這個漏洞，在用戶 WordPress 的安裝主目錄中新增一個含有任意惡意程式碼的檔案，並可遠端執行。

第一個漏洞的 CVSS 危險程度評分高達 9.0 分，屬於嚴重（Critital）等級；目前暫無 CVE 編號。

第二個漏洞則是屬於跨站連線要求偽造（cross-site request forgery, CSRF）；駭侵者可透過這個漏洞，發送偽造的連線要求，改寫受害者的設定值，將受害者安裝的 Facebook for WordPress 像素追蹤資料改為發送到攻擊者端，這樣便能竊取受害 WordPress 網站的流量統計資訊；駭侵者甚至還能進一步注入惡意 JavaScript，遠端執行任意程式碼。

這個漏洞的 CVSS 危險程度評分高達 8.8 分，屬於高危險（High）等級；目前暫無 CVE 編號。

這兩個漏洞均已在近期推出的 Facebook for WordPress 3.0.4 中修復；有安裝此擴充套件的用戶，均應立即更新到 3.0.4 以上版本，以降低網站被駭的風險。

- 影響產品/版本：Facebook for WordPress 2.2.2 或先前版本（PHP 物件注入漏洞）；3.0.0-3.0.3（CSRF 漏洞）
- 解決方案：升級到 3.0.4 或之後的版本

- 資料來源：
  1. Two Vulnerabilities Patched in Facebook for WordPress Plugin
  2. Severe vulnerabilities patched in Facebook for WordPress Plugin

2.7.4、Adobe 修復 Creative Cloud、Adobe Connect 及 Framemaker 的漏洞

Adobe 於 2021 年 3 月 9 日發布了安全性更新，修復存於 Adobe Creative Cloud Desktop、Connect 和 Framemaker 的資安漏洞。

Adobe 修復了 1 個 Adobe Framemaker 遠端執行任意程式碼漏洞、3 個 Adobe Creative Cloud Desktop 嚴重漏洞，以及 4 個 Adobe Connect 的資安漏洞，共修復了 8 個漏洞，大部分漏洞因允許遠端執行任意程式碼，故被評為嚴重等級。

其中 Adobe Creative Cloud Desktop 修復了三個漏洞，包含兩個允許遠端執行任意程式碼漏洞和一個特權提升漏洞。遠端執行任意程式碼是屬於較嚴重的漏洞，駭侵者能夠執行 Windows 命令，並安裝惡意軟體或是接管用戶電腦。

Adobe 建議使用以上相關產品之用戶盡快更新至最新版本，以防止舊版本的漏洞被駭侵者利用而遭到攻擊。

- 影響產品/版本：
  1. Creative Cloud Desktop Application 5.3 及更早之前之版本。
  2. Adobe Connect 11.0.5 及更早之前之版本。

3. Adobe Framemaker 2019.0.8 及之前的版本。

- 解決方案：將以上產品更新至最新版本

- 資料來源：
  1. Adobe fixes critical Creative Cloud, Adobe Connect vulnerabilities
  2. Security update available for Adobe Creative Cloud Desktop Application | APSB21-18
  3. Security updates available for Adobe Connect | APSB21-19
  4. Security Updates Available for Adobe Framemaker | APSB21-14

2.7.5、網路設備廠商 F5 呼籲用戶修補 BIG-IP 與 BIG-IQ 產品的嚴重漏洞

F5 Networks BIG-IP 與 BIG-IQ 產品存有多個資安漏洞，允許駭侵者遠端執行任意程式碼，建議相關產品用戶更新至已修復版本。

網路和網安設備廠商 F5 Networks 發布了安全性更新，共 7 個漏洞，影響多數 BIG-IP 和 BIG-IQ 版本，其中包含四個嚴重的遠端執行任意程式碼(Remote Code Execution, RCE)漏洞。

四個嚴重 RCE 漏洞中一個屬於預授權 RCE 漏洞(CVE-2021-22986)，此漏洞使未經身分驗證的遠端駭侵者可以在被入侵的 BIG-IP 設備上執行任意代碼，CVSS 評分 9.8 分。

其餘三個嚴重漏洞分別為：

1. 流量管理用戶介面(Traffic Management User Interface, TMUI)在未公開的頁面中存在具有身分驗證的 RCE 漏洞(CVE-2021-22987)，CVSS 評分高達 9.9 分。
2. 流量管理微核心(Traffic Management Microkernel,TMM)存在緩衝區溢位漏洞(CVE-2021-22991)，CVSS 評分 9.0 分。
3. Advanced WAF/ASM 存有緩衝區溢位漏洞(CVE-2021-22992)，CVSS 評分 9.0 分。

2021 年 3 月 10 日，F5 又發佈了另外 3 個 RCE 漏洞的安全公告（2 個高度風險 CVE-2021-22988、CVE-2021-22989，1 個中度風險 CVE-2021-22990，其 CVSS 評分分別為 8.8、8.0、6.6），允許經過驗證的遠端攻擊者執行任意系統命令。BIG-IP 的 RCE 漏洞可能會導致全面的系統入侵，包括截取控制器應用流量和橫向移動到內部網路。

根據 F5 的資訊，這 7 個漏洞在以下 BIG-IP 版本中已得到修復：16.0.1.1、15.1.2.1、14.1.4、13.1.3.6、12.1.5.3 和 11.6.5.3。影響 BIG-IQ 的預授權 RCE 漏洞(CVE-2021-22986)也在 8.0.0、7.1.0.3 和 7.0.0.2 版本中均已修復。

F5 在 BIG-IP 升級指南詳細介紹了多種升級方案，並呼籲相關產品用戶盡快進行漏洞修補更新。

- CVE 編號：CVE-2021-22986、CVE-2021-22987、CVE-2021-22988、CVE-2021-22989、CVE-2021-22990、CVE-2021-22991、CVE-2021-22992
- 影響產品/版本：BIG-IP 與 BIG-IQ 的多個版本
- 解決方案：依照 F5 官方提供之升級指南，將受影響產品更新至已修復版本。

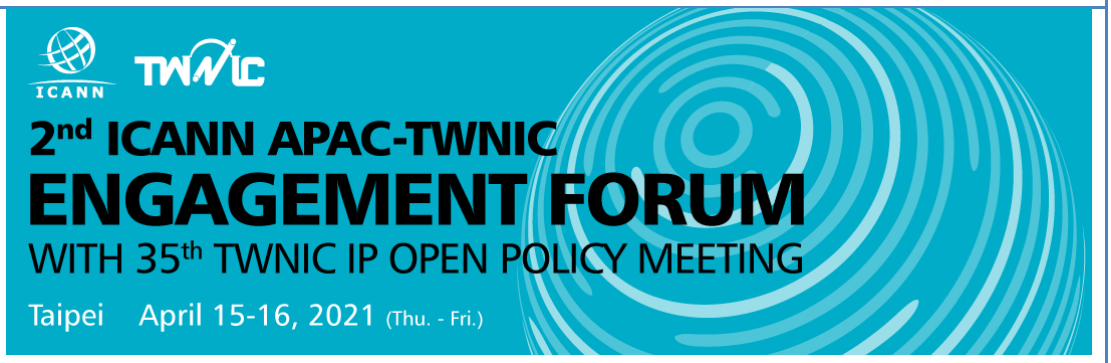
- 資料來源：
  1. K84205182: BIG-IP update and upgrade guide | Chapter 1: Guide contents
  2. K03009991: iControl REST unauthenticated remote command execution vulnerability CVE-2021-22986
  3. K18132488: Appliance mode TMUI authenticated remote command execution vulnerability CVE-2021-22987
  4. K56715231: TMM buffer-overflow vulnerability CVE-2021-22991
  5. K52510511: Advanced WAF/ASM buffer-overflow vulnerability CVE-2021-22992

6. F5 urges customers to patch critical BIG-IP pre-auth RCE bug

7. F5 Networks 之 BIG-IP 產品與 BIG-IQ 產品存在安全漏洞

第 3 章、 資安研討會及活動

資安事故處理實務探討	
活動時間	**2021-04-14 09:00 ~ 17:00**
活動地點	**協志聯合攻防中心(台北市中山區中山北路三段 22 號)**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjYwNg==**
活動概要	 **主辦單位：中華民國資訊軟體協會** 聯絡窗口： 0225533988 分機 358　溫專員　alisa.wen@cisanet.org.tw 報名截止： 2021-04-12 課程內容： 端點勒索軟體與 APT、網站入侵、雲端線上服務、行動與物聯網裝置、資料庫和資料外洩等事故案件解析。

第二屆 ICANN APAC-TWNIC Engagement Forum 與第 35 屆 TWNIC IP 政策資源管理會議	
活動時間	**2021 年 4 月 15 與 16 日**
活動地點	**台北福華大飯店地下二樓福華廳**
活動網站	**https://forum.twnic.tw/2021/**
活動概要	 **主辦單位：ICANN、TWNIC** ICANN 及 TWNIC 共同舉辦合作交流論壇 (ICANN APNIC-TWNIC Engagement Forum)，集合了網路相關利害關係人與國際相關網路社群，針對域名、IP 位址及網路安全等主題，進行深入議題探討，這將是台灣與國際網路利害關係人共同面對面討論全球網路議題的最佳機會。 第 35 屆 TWNIC IP 政策資源管理會議希望促進網際網路相關產業發展為目標之會議，提供各界有關網路技術研究、產業發展之溝通交流平台，彙集臺灣地區各 ISP 業者之意見提供相關 IP 政策及管理機制。 ICANN 及 TWNIC 建立論壇平台，讓地區內之網路相關利害關係人，可以藉由合作交流論壇從區域及台灣的角度探索政策、科技與協作等不同面向中各方利害關係人的觀點。

政府受駭案例與因應	
活動時間	**2021-04-15 18:30 ~ 21:30**
活動地點	**協志聯合攻防中心(台北市中山區中山北路三段 22 號)**
活動網站	**https://www.cisanet.org.tw/News/activity_more?id=MjYwMQ==**
活動概要	 **主辦單位：中華民國資訊軟體協會** 聯絡窗口： 0225533988 分機 358　溫專員　alisa.wen@cisanet.org.tw 報名截止： 2021-04-12 課程大綱： ● 政府企業資安威脅種類 ● 資安攻擊入侵思維 ● 實際案例 1 ：我國重要油品事業近期遭勒索病毒案 ● 實際案例 2 ：其它政府機關遭駭客入侵案 ● 個人資安防護議題

CYBERSEC 2021 臺灣資安大會	
活動時間	**5/4 (二) ~ 5/6 (四)**
活動地點	**南港展覽二館**
活動網站	**https://cyber.ithome.com.tw/**
活動概要	 **主辦單位：iThome** 2020 年 8 月疫中的臺灣資安大會，我們見證了上萬名與會者發揮臺灣最傲人的公民水準，一起貫徹防疫最高指導原則，讓臺灣年度資安盛事既安全又圓滿地達成；也由於大家的努力，臺灣資安業界一年一度的交流盛會不僅沒有被疫情打倒，更因為臺灣全國上下一心的防疫成果，讓臺灣資安大會成為年度全球唯二正常舉辦的資安會議。 今年，雖然全球疫情依然嚴峻，然而臺灣上下仍堅持住防疫作為，防疫成果持續傲視全球，因此我們有理由相信在大家遵守中央流行疫情指揮中心最高防疫準則下，2021 年 5 月能夠再次成功舉辦臺灣資安大會，讓全球繼續看見臺灣的韌性。 而且，今年很可惜的是，全球最大的資安會議已經因為疫情嚴峻而取消實體活動，因此 2021 年臺灣資安大會極有可能成為全球唯一能夠實體舉辦的資安會議。所以，這次臺灣更是任重道遠，我們一定要撐住全球的資安會議。 聯絡資訊：CYBERSEC 2021 臺灣資安大會服務小組 cybersec@ithome.tw

第 4 章、 2021 年 3 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。

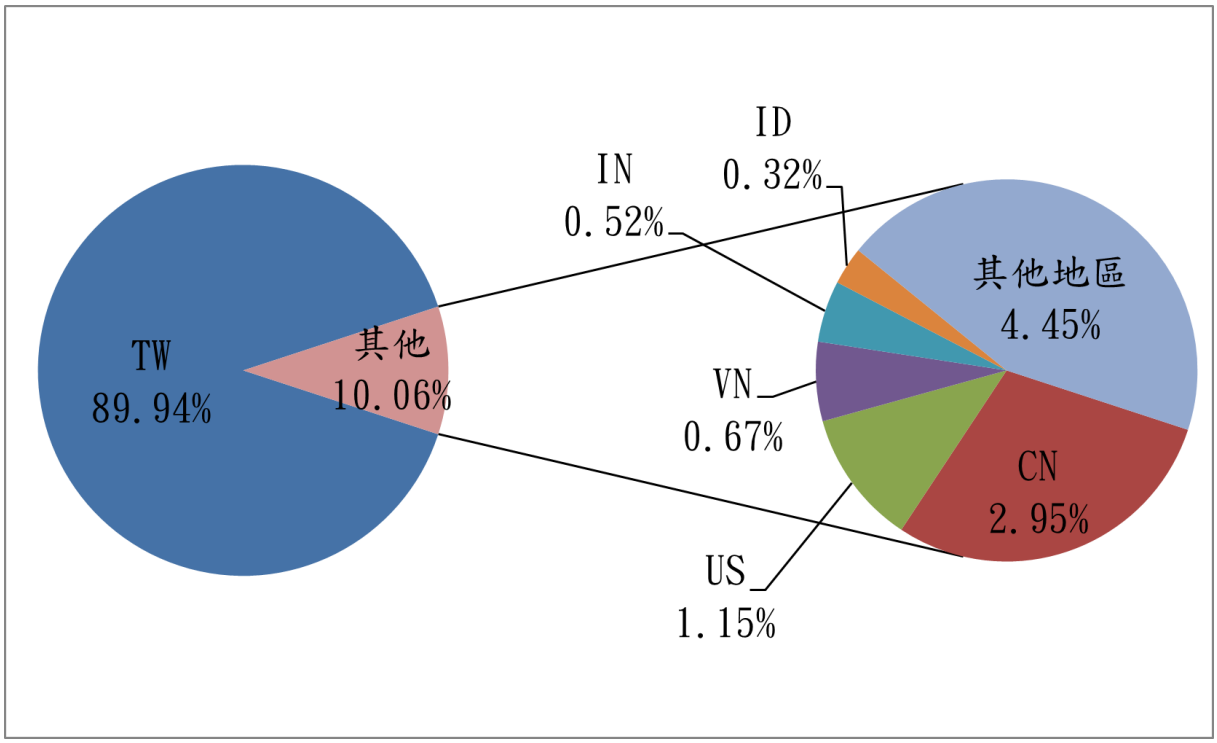


圖 1、分享地區統計圖

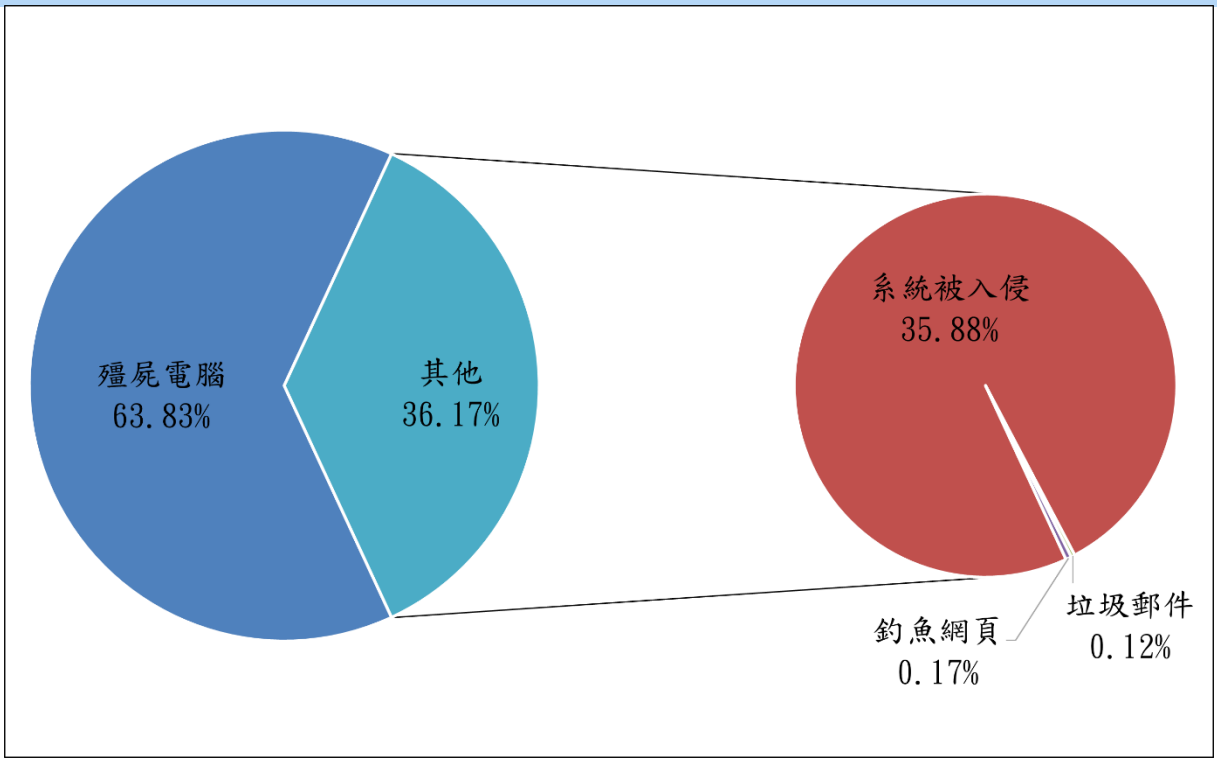


圖 2、分享類型統計圖

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：**2021 年 4 月 10 日**

編輯：**TWCERT/CC 團隊**

服務電話：**0800-885-066**

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**