# TWCERT/CC 資安情資電子報

## 2020 年 4 月份

# 目錄

# 第 1 章、 封面故事

## Windows 被發現全新漏洞，利用此漏洞的惡意程式感染率高，請立即更新


**這個漏洞存在於 Microsoft Server Message Block (SMB) 協定 3.1.1 版本，亦稱為 SMBv3，用來在內部網路與 Internet 上的電腦、印表機、其他連網裝置間進行各種資料交換與分享。**

CVE-2020-0796 這個資安漏洞，就是透過發送特殊封包給 SMBv3，即可在 SMB Server 或其他 SMB Client 上執行任意程式碼。該漏洞影響 1903 / 1909 版本的 Windows 10 和 Windows Server。

在思科資安團隊先前發表過的研究報告中，用了「Wormable」這個字來形容本漏洞，意思是指透過這個漏洞進行的駭侵攻擊，可以直接在網路間感染一台又一台的未修補裝置，不需要和任何實際的管理者或使用者互動。

在這份被撤回的文件中也說，尚未進行安全更新的用戶，最好事先在防火牆和其他設備上關閉 SMBv3 使用的 TCP 通訊埠 445，以防利用這個漏洞的惡意軟體在網路上到處流竄。

據微軟表示，目前還沒有觀察到利用這個漏洞進行的大規模駭侵攻擊事件。用戶可先關閉 SMBv3 壓縮，同時在企業的防火牆上封鎖 TCP 連接埠 445；但這只能防範來自外網的攻擊，如果內網已有電腦感染，此法無效。

- 建議措施

由於此漏洞會產生加密勒索蠕蟲流竄，GitHub 等網站也逐漸釋出 PoC 範例程式碼，駭客可能會將此範例程式碼改為蠕蟲化的加密勒索惡意程式，攻擊國內企業與政府電腦等 IoT 設備，造成資安威脅。因此根據中華民國網路封包分析協會的建議，採取以下防護措施：

1、 為阻斷外部網路的網路蠕蟲攻擊，請關閉網路防火牆 TCP-445 的通訊埠。另外為避免用戶端感染 SMBv3 蠕蟲的電腦，透過 VPN 攻擊內部電腦，請暫時禁止用戶端在 VPN 使用 TCP-445。

2、 關閉會攜帶外出並使用外部網路公務筆電的有限及無線網路 Microsoft Network 功能支援，停用 Netbios Over TCP/IP 功能。

3、 立即進行安全性更新，以修補資安漏洞。

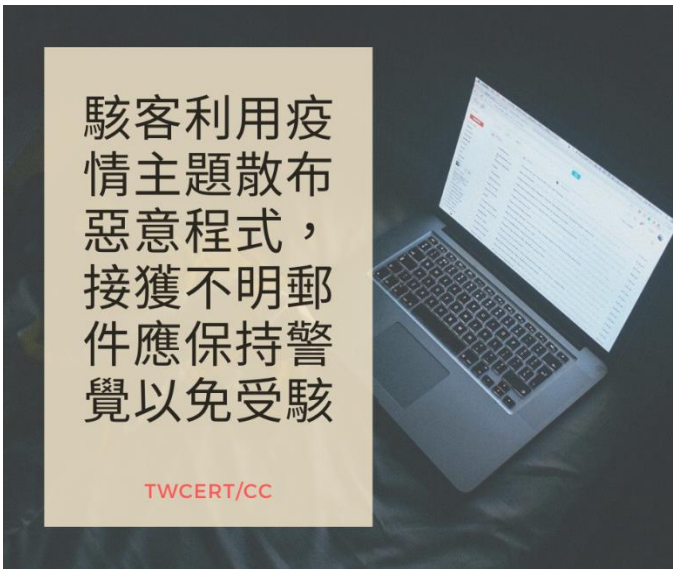
- CVE 編號：CVE-2020-0796
- 影響版本：Windows 10（版本 1903、1909)、Windows Server（1903、1909）
- 解決方案：更新至最新版本

- 資料來源：
  1. https://nvd.nist.gov/vuln/detail/CVE-2020-0796
  2. https://www.helpnetsecurity.com/2020/03/11/cve-2020-0796/
  3. https://arstechnica.com/information-technology/2020/03/windows-has-a-new-wormable-vulnerability-and-theres-no-patch-in-sight/
  4. https://www.bleepingcomputer.com/news/security/48k-windows-hosts-vulnerable-to-smbghost-cve-2020-0796-rce-attacks/
  5. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
  6. https://www.nspa-cert-tw.org/

# 第 2 章、 國內外重要資安事件

## 2.1、資安趨勢

### 2.1.1、駭客利用疫情主題散布惡意程式，接獲不明郵件應保持警覺以免受駭




**由於 COVID-19(新冠肺炎、武漢肺炎)疫情的蔓延，許多 APT 駭侵組織或有心人士利用相關內容，散布以此為主題的釣魚郵件。**

資安人員 PARTHI 發現 APT 組織 MustangPanda 以 COVID-19 疫情為誘餌，發送假冒政治人物發言且含有惡意附件的電子郵件。其中假冒政治人物的文檔為冒充我國副總統陳建仁，內容聲稱副總統在臉書說明 COVID-19 社區傳播的特性以及台灣沒有發生社區傳播，還提到美國疾病管制與預防中心列出有社區傳播風險的目的地就包含台灣，如上圖所示。

該電子郵件附檔是含有惡意程式碼的文件，透過 mshta.exe 執行，執行後出現冒充副總統發言的文檔以及一個惡意執行檔。惡意執行檔會執行另一個內含三個惡意檔案。執行時，該惡意檔案內的三個檔案會被放入使用者電腦的 Music 文件夾中，其中一個是假冒知名影音軟體名稱及圖示的檔案，藉此讓使用者信以為真誘導點擊，點擊後將會執行其他兩個惡意檔案，並連結到駭客掌控的 C&C 伺服器下載並植入 Cobalt Strike 等攻擊工具至受害者電腦，進行盜錄鍵盤和螢幕畫面，以及下載檔案等惡意行為，並成為殭屍電腦(Bot)。

與 2020 年 1 月利用 COVID-19 名義的釣魚郵件不同，前者主要是針對日本等當時 COVID-19 疫情較嚴重的國家，以武漢肺炎名義傳播 Emotet 類型的惡意巨集電郵，信件中提及其附件為政府相關衛生單位提供之防疫措施，以此誘使使用者點擊附件，造成憑證及瀏覽紀錄等相關資訊遭惡意程式竊取。而此次攻擊同樣以 COVID-19 疫情為餌發送釣魚郵件，郵件發送對象針對台灣與越南，內容是冒充各國政治人物的聲明或是防疫相關建議，使關心疫情狀況的民眾上當點擊，進而在受害者電腦植入惡意程式，成為殭屍電腦。除了以上針對日本、台灣及越南的釣魚郵件之外，世界各國皆有受到駭侵組織或駭客以此波疫情為主題，誘導民眾開啟的釣魚郵件攻擊，目的是誘使用戶點按惡意連結或附檔，來植入惡意程式。因此當收到 COVID-19 疫情相關電郵，應特別注意並警覺，以免上當受害。

自 COVID-19 疫情爆發以來，除了電子郵件惡意活動外，專家還發現大量新網站註冊了與該病毒相關的網域名稱，其中，有多個網域名稱可能被用於網路釣魚，這些網站會利用新型冠狀病毒相關討論引誘受害者進入，還有一些詐騙網站聲稱會出售口罩、疫苗和居家病毒檢測試劑。建議民眾避免進入可疑網站及留下個資，以免造成個人損失。

建議使用者收到電子郵件時，對寄件人進行身分確認，若收到需要點擊連結或下載附件之郵件，在未確認寄件人身分之前或是針對標題及內容可疑的信件，不隨意點擊任何信件中的連結、不開啟不下載郵件中夾帶的附件，以免遭駭客入侵使電腦被植入惡意程式。進入可疑網站不隨意輸入帳密和個資，確認網址的正確性，可以使用網址識別套件或直接在瀏覽器手動鍵入網址，防止進入釣魚網站。TWCERT/CC 發現此類網安威脅後，已將相關情資藉由我國資安情資分享系統通知國內主要 ISAC 單位，請民眾若收到新冠肺炎疫情相關釣魚郵件不須特別驚慌，依照以上建議方案並查證郵件真實性，即不需要擔心受到駭客攻擊而造成損失。

- 資料來源：
  1. https://malwareandstuff.com/mustang-panda-joins-the-covid19-bandwagon/
  2. https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication
  3. https://twitter.com/cyber__sloth/status/1232977498784354304
  4. https://www.twcert.org.tw/tw/cp-104-3286-aeae8-1.html

## 2.1.2、80% 資安駭侵攻擊假借 COVID-19 為名發動


**資安廠商發表監控報告，指出近來觀察到的各式駭侵攻擊活動，有八成都假借 COVID-19(新冠肺炎、武漢肺炎)名義進行。**

資安廠商 Proofpoint 上周發表監控報告，指出近來觀察到的各式駭侵攻擊活動，有八成以上的案例，都假借 COVID-19 名義進行。

這類假借 COVID-19 為名，企圖混淆視聽，吸引受害者上鉤的駭侵活動，有些直接在主題或其內容使用肺炎疫情，有些雖然沒有直接使用，但在連結或附件中也使用了肺炎疫情的各式名義。

Proofpoint 監測 140 個以上不同的這類假借肺炎疫情進行的駭侵攻擊行為，記錄到超過五十萬封釣魚信件、三十萬個惡意連結，以及二十萬個有害的附件檔案；攻擊型態也是五花八門，從企圖駭入中小企業內部的釣魚信件外，還包括企圖騙取登入資訊、直接置入惡意軟體的郵件，或是單純的垃圾信等。

Proofpoint 說，這些攻擊中最常見的，還是企圖騙取登入資訊的釣魚信件；而發動這些駭侵攻擊的駭侵者，除了類似 TA542（Emotet 惡意軟體的幕後勢力）之外，也包括各類中小型駭侵組織或個人。

Proofpoint 也列出數個常見的釣魚信件主題，包括「本公司有人感染肺炎」、「你的鄰居有人感染」、「WHO 宣布找到肺炎解藥」、「申請滅菌金融卡」等等，其主題還會隨著社會大眾不同的關心話題而變化。

Proofprint 指出，隨著全球疫情的持續升溫，民眾對疫情的恐慌與日俱增，這類假借疫情而進行的駭侵攻擊也會更為猖獗。

- 資料來源：
  1. https://www.proofpoint.com/us/threat-insight/post/threat-snapshot-coronavirus-related-lures-comprise-more-80-percent-threat
  2. https://securitybrief.eu/story/80-of-cyber-threat-landscape-uses-covid-19-as-leverage-report

## 2.1.3、各國駭侵團體利用 COVID-19 疫情恐慌，攻擊 Windows 用戶


**資安廠商偵測到各國駭侵團體，利用全球對 COVID-19(新冠肺炎、武漢肺炎)大流行的恐慌，以提供防疫說明文件形式，夾帶惡意軟體的大量攻擊案件。**

資安廠商 Check Point 發表監測研究報告，指出該公司觀察到有 APT 駭侵組織利用偽造的蒙古國外交部說明 COVID-19 防治的新聞稿，在其中夾藏惡意軟體並透過社交工程與釣魚攻擊，試圖駭侵蒙古國各政府部門。

無獨有偶，另一家資安廠商 Red Drop 也在日前發現另一個駭侵組織，以類似的手法，用偽造印度政府新聞稿的方式，試圖攻擊印度軍事與情報單位。

資安廠商 Malwarebyte 指出，駭侵團體 APT36 鎖定的是透過 RTF 夾檔，利用已知的 Windows 漏洞 CVE-2017-0199，讓駭侵者可以遠端執行任意程式碼。

英國國家資安中心（NCSC）則警告大眾，有愈來愈多國家的一般人民，最近開始收到內含惡意軟體的 COVID-19 病毒相關釣魚信。NCSC 指出，這些信件中多半以內含重要更新訊息為餌，誘使用戶點按惡意連結；大眾應該特別提高警覺。

據富比士報導，這些被發現利用疫情恐慌發動的攻擊，不過只是冰山一角；未來還會有更多駭侵者利用這波疫情，向急於獲悉情報或解方的大眾發動各式駭侵攻擊，用以取得機敏資訊或牟取不法利益。

- 資料來源：
  1. https://www.forbes.com/sites/zakdoffman/2020/03/12/chinese-hackers-weaponized-coronavirus-data-to-launch-this-new-cyber-attack/#308d58be3861
  2. https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus
  3. https://twitter.com/RedDrip7/status/1237983760802394112

## 2.1.4、大批工作者在家遠距上班，各種資安威脅因之加劇


**美國因疫情實施大規模遠距工作，各種資安威脅的壓力也隨之升高；包括資安防護、防範數位犯罪的需求也大為增加。**

美國因疫情實施大規模遠距工作，資安官員與專家紛紛指出，各種資安威脅的壓力也隨之升高；包括資安防護、防範數位犯罪或網路攻擊的需求，也大為增加。

據美國之音報導，美國聯邦調查局（FBI）和多家資安廠商都已觀察到愈來愈密集的網路攻擊行動，包括假冒防疫單位寄出的釣魚郵件、試圖趁亂進行的社交工程詐騙等。

不少釣魚信件會偽裝成像是由美國疾病管制中心（U.S. Centers for Desease Control and Prevention）或世界衛生組織 WHO 發布的警訊，利用社會大眾的恐慌心理，誘使受害者點擊信件中的惡意連結，或含有惡意程式碼的附件。

資安廠商 ProofPoint 的資深研究主任 Sherrod DeGrippo 指出，該公司觀察到的最大宗釣魚郵件攻擊行動，一口氣就寄發了三十萬封攻擊郵件；他預期很快就會出現不同的變種攻擊案例。

DeGrippo 也指出，在家遠距工作者，經常是使用個人的電腦設備，透過 VPN 連上各公司的內部網路；通常這類個人設備的資安防護能力，較一般辦公室內的資訊設備為低，因此也比較不易阻擋各種資安威脅。

另外，由於大量工作者遠距上班時，係透過自己家中的寬頻網路或手機無線上網，也對電信基礎設施造成連線壓力；駭侵者只要攻擊這些基礎設施，就能造成比平常更大的破壞，讓大量遠距上班者無法透過網路工作。

- 資料來源：
  1. https://twitter.com/CISAgov/status/1240349548402401283
  2. https://twitter.com/FBIWFO/status/1239591031034830848
  3. https://www.voanews.com/science-health/coronavirus-outbreak/cyber-threat-increases-more-americans-telework。

## 2.1.5、八百萬筆歐洲區 Amazon 和 eBay 等大型電商顧客交易資料遭曝光


**資安專家在網路發現一個未受保護的大型資料庫，內含數百萬名歐洲 eBay 和 Amazon 等大型電商業者顧客的各種資料，而且只要用搜尋引擎就可以找到。**

資安廠商 Comparitch 的專家 Bob Diachenko 指出，這個資料庫中的資料多達八百萬筆交易資料，主要是透過 Amazon、eBay、Shopify、PayPal、Stripe 等電商或數位支付業者提供的 API 收集。

專家表示，這個存在 AWS 上的 MongoDB 資料庫，並未加上任何保護措施；當今年 2 月 3 日時被發現後，一直在網路上放了五天才撤下；在這段期間，任何人都可以透過簡單的網路搜尋找到這個資料庫。

由於一名顧客可能產生多筆交易資料，所以目前不易估計受影響人數的規模；但其中有一半的資料是來自英國的顧客，其他的來自歐洲其他國家。

據 Comparitech 公司的分析，製作這個資料庫的，可能是一家進行跨境加值型營業稅分析的第三方公司。目前沒有證據指出這個資料庫在曝光期間曾遭到任何不當存取，Amazon 在接獲通報後，也已展開調查，而可能涉及製作該資料庫的第三方公司，則在 2 月 8 日自網路上撤下了這個資料庫。

- 資料來源：
  1. https://www.comparitech.com/blog/information-security/uk-shopper-records-exposed/
  2. https://nakedsecurity.sophos.com/2020/03/12/data-of-millions-of-ebay-and-amazon-shoppers-exposed/

## 2.1.6、英國資安公司洩露超過五十億組登入資訊


**一個全無保護，由一家英國資安公司擁有，含有五十億組登入資訊的 Elasticsearch 資料庫，在網路上被發現。**

今年二月時，有一組內含 22 億組登入資訊的未受保護資料庫在網路上被發現；事隔僅一個月，資安專家再次發現一個更大的登入資訊資料庫，同樣未受保護，可供人任意存取。

涉及洩露這個龐大資料庫的，是一家位在英國的資安公司，名為 Keepnet Labs；發現這個資料庫的，是著名的獨立資安研究人員 Bob Diachenko。他根據這個資料庫的 DNS 記錄與 SSL 憑證資訊，追出 Keepnet Labs 這場資安事件。

資料庫中收集的登入資訊，主要來自 2012 年到 2019 年間，針對 Twitter、Tumblr、Adobe、Vk、LinkedIn、Last.fm 等服務的各項大規模攻擊駭侵事件中流出的帳號密碼，共分成兩個檔案；第一個檔案含有五十億筆記錄，第二個檔案雖然只含一千五百萬筆記錄，但卻有即時更新。

資料庫中的欄位，主要包括加密過與未加密的密碼、雜湊類型、Email 網域、Email 地址、資料洩漏日期與來源等。

Diachenko 指出，雖然這個資料庫中的登入資訊，大多是以前就已洩露過的，但對資料失主來說，是又一次的傷害，因為這對意圖進行釣魚攻擊的駭侵者來說，是難得一見的極佳資料來源。

Diachenko 在發現這個資料庫後，第一時間就向 Keepnet Labs 發出通報，而這家公司也立即撤下資料庫。

- 資料來源：
  1. https://securitydiscovery.com/data-breach-database-data-breach/
  2. https://www.securitymagazine.com/articles/91970-uk-based-security-company-exposes-database-containing-more-than-5-billion-records

## 2.1.7、東南亞多國發生大規模信用卡資料外洩事件，資料外洩卡量近 32 萬張


**東南亞多個國家發生多起信用卡資料遭外洩事件，共有多達近 32 萬張卡片資訊遭竊；受影響國家包括新加坡、馬來西亞、菲律賓、越南、印尼、泰國。**

印度資安新創公司 Technisanct 發表研究報告，指出至少六個東南亞國家的大批信用卡資料遭到駭侵者竊取，包括信用卡有效期限、CVV 安全碼和用戶的可識別個人資訊均遭外洩。

該公司指出，在外洩的近 32 萬張信用卡中，受害最深的是菲律賓，共有超過 17 萬張信用卡資訊外洩；馬來西亞有三萬七千多張，新加坡則有兩萬五千張左右。

該公司表示，發現有大量信用卡資訊，被駭侵者在暗網上販售。由於這些資料除了卡號外，還有信用卡安全碼和用戶的個資，所以很容易用來盜刷。儘管有些刷卡機制需要進行二階段驗證（例如輸入簡訊傳遞的隨機安全碼），但還是有很多交易場合缺少這類額外的安控機制。

該公司在發現此一事件後，立即以 Email 通報各國的資安緊急事件處理單位（CERT），並建議各國 CERT 立即採取行動，以免災情擴大，但至今沒有一個國家對此發表回應。

南華早報就此事採訪馬來西亞官方資安主管機關、中央銀行、金融主管機關等。

馬來西亞第二大的聯昌國際銀行（CIMB Group Holdings）向南華早報表示，該行沒有發現被入侵導致資料外洩的具體情事。

- 資料來源：
  1. https://www.technisanct.com/press-release.php
  2. https://www.scmp.com/week-asia/article/3073848/singapore-malaysia-credit-card-details-dumped-online-massive-data-breach。

## 2.1.8、Tesla 與 SpaceX 零組件供應商遭駭侵攻擊


**一家為 Tesla 與 SpaceX 製造精密零組件的廠商，遭到勒贖軟體駭侵攻擊。**

這間遭駭的廠商名為 Visser Precision，位在美國科羅拉多州的丹佛市，除了為 Tesla 和 SpaceX 製造多種精密零組件外，客戶也包括其他的汽車製造業、航太產業與國防工業。

據 TechCrunch 報導，該公司證實最近發生資安事故，公司所屬的資料可能遭到不當存取，甚至被竊；該公司正在加緊調查事件，不過公司的運作如常，並未受到影響。

資安專家指出，Visser 係遭到一個名叫「DoppelPlaymer」的勒贖軟體攻擊；這個惡意軟體的攻擊方式，有別於傳統勒贖軟體。DoppelPlaymer 在加密資料前會先匯出資料，並且威脅受害者，如果不支付贖款，被竊取的機敏資料即將遭到公開。

Emsisoft 的資安專家表示，Visser 被竊的資料已在某網站遭到公開；其資料顯示許多該公司客戶的名稱，包括 Tesla、SpaceX、波音公司、洛克希德馬丁公司等汽車、航太、國防工業等業者；外洩的檔案包括 Visser 與客戶簽訂的保密條款，以及某些飛彈通訊天線架構的部分設計資料。

據資安專家指出，DoppelPaymer 最近的一系列駭侵攻擊，造成多家公司資料外洩並被竊；除了這次的 Visser Precision 外，去年十二月一家名為 Allied Universal 的保全公司，也因為拒付 230 萬美元的贖金，其公司內部機敏資料亦被公開。

- 資料來源：
  1. https://www.forbes.com/sites/daveywinder/2020/03/02/lockheed-martin-spacex-and-tesla-caught-in-cyber-attack-crossfire/#5c598ceb7b2d
  2. https://techcrunch.com/2020/03/01/visser-breach/

## 2.1.9、美國與香港電信業者遭全新僵屍模組的暴力 RDP 連線攻擊


**資安廠商發現一個全新的 TrickBot 模組，針對美國和香港的特定業者發動暴力 RDP 連線攻擊。**

資安廠商 BitDefender 的研究人員，發現一個全新的 TrickBot 模組 rdpScanDll，開始針對美國和香港的特定業者，發動暴力 RDP 連線攻擊。

BitDefender 是在今年一月三十日時發現全新 TrickBot 的攻擊行動；根據其攻擊的 IP 進行分析，發現主要的攻擊目標，是美國和香港的電信業者。

一般來說，典型的 TrickBot 攻擊是在 2016 年開始出現的，當時以數位銀行的登入資訊取得為主要的攻擊目的，但近年其攻擊範圍和樣態也開始增加，不但新增了多種新功能，被攻擊的目標對象也擴及金融業之外的其他業種。

BitDefender 指出，目前觀測到的 TrickBot 和 rdpScalDll，會針對目標對象，以暴力嘗試法試圖連入受害者的 RDP 遠端桌面，以取得控制權；他們也發現主要控制這些僵屍模組的控制伺服器多半位在俄羅斯，而且每個月會新增約一百台控制伺服器的 IP，每次的攻擊區間約持續 16 日之久。

這些僵屍網路攻擊模組，主要透過垃圾郵件散布，但最近也觀測到駭侵者透過其他管道散布。

除了電信業者外，BitDefender 也觀測到香港與美國的教育機構、金融服務業等業種，也受到這個駭侵攻擊的威脅。

由於這個攻擊模組的架構，可以加掛各種攻擊用的外掛套件，所以相當具有彈性，可以根據駭侵者的需求，進行各種調整和修改，結果就是這個模組出現很多複雜和先進的變種，攻擊的樣態和目標也變得更為多元。

- 資料來源：
  1. https://www.bitdefender.com/files/News/CaseStudies/study/316/Bitdefender-Whitepaper-TrickBot-en-EN-interactive.pdf
  2. https://labs.bitdefender.com/2020/03/new-trickbot-module-bruteforces-rdp-connections-targets-select-telecommunication-services-in-us-and-hong-kong/

## 2.1.10、專家警告，全美眾多連網醫療裝置，因多種原因易遭駭


**據一份最新研究報告指出，全美有大量可連網之醫療用裝置，因為包括資安防護配置不當、作業系統老舊等原因，曝露在駭侵攻擊的風險之下。**

資安廠商 PaloAlto Networks 的資安研究人員，日前發表研究報告，指出全美國有眾多連網醫療器材與裝置，因為各種不當資安配置，或作業系統版本過於老舊，因而曝露在極高駭侵攻擊風險之下。

這項研究分析全美上千家醫療院所中的 120 萬台醫療相關 IoT 裝置。報告指出，有 83% 的醫用影像裝置仍執行在老舊且已失去原廠支援的作業系統，其中 56% 執行 Windows 7，11% 執行 Windows XP；仍保有原廠支援的裝置數量比例僅有 17%。

另外，有高達 98% 的醫療廠所，其 IoT 裝置的網路通訊內容並未加密；72% 醫療場所的內部網路，將各種醫療器材與一般 IoT 裝置混用，而這些 IoT 裝置中又有 57% 含有中等程度以上的資安漏洞尚未修補。

報告也分析過去針對醫療院所發動的駭侵攻擊，指出有 41% 的攻擊行動鎖定這些裝置的資安漏洞發動駭侵，另外有 51% 的駭侵攻擊和醫療影像裝置有關。

進一步細分攻擊的類型，除了上述 41% 的攻擊鎖定裝置漏洞外，有 33% 以惡意軟體發動攻擊，另外 26% 則針對使用者的操作疏失發動攻擊，如釣魚郵件

等。

- 資料來源：
  1. https://unit42.paloaltonetworks.com/iot-threat-report-2020/
  2. https://venturebeat.com/2020/03/10/more-good-news-medical-equipment-is-still-prone-to-hacker-attacks/

## 2.2、行動裝置資安訊息

### 2.2.1、惡意 APP 破解雙因子驗證，竊取交易認證碼


**2020 年 3 月 IBM X-Force 研究人員分析了由 TrickBot 傳播的惡意 Android 應用程式 TrickMo。**

2019 年 9 月 CERT-Bund 研究人員發現 TrickBot 駭侵團體擁有知名銀行木馬，並使用中間人攻擊以取得用戶的手機號碼與設備類型等資訊。確認用戶使用 Android 作業系統後，此木馬便會冒充其銀行，誘使用戶下載並安裝以保護帳戶的假防毒軟體等安全應用程式，如偽冒 Avast Security Control APP 或 Deutsche Bank Security Control APP。假冒的安全應用程式其目的在於獲取用戶的交易驗證碼，以登入用戶的網路銀行。

2020 年 3 月 IBM X-Force 研究人員分析了由 TrickBot 傳播的惡意 Android 應用程式 TrickMo。TrickBot 駭侵團體使用其開發的惡意應用程式 TrickMo，竊取用戶交易驗證碼（Transaction Authentication Number, TAN）後繞過銀行使用的雙因子驗證 (Two-Factor Authentication, 2FA)保護。TrickMo 的目的是攔截銀行透過簡訊或推播通知發送給用戶的一次性密碼(One-Time Password, OTP)，並傳送回駭侵團體控制的 C&C 伺服器。TrickMo 是竊取交易驗證碼最新的變種，可以被使用在任何地區的銀行。

當用戶安裝 TrickMo 至 Android 設備，該惡意應用程式會將自己設置為預設的簡訊應用程式，以此攔截設備上的任何簡訊，包含一次性密碼、mobile TAN (mTAN)等交易驗證碼。若銀行進行安全性升級，不使用基於簡訊發送的驗證方

式而改用銀行應用程式藉由推播通知發送交易驗證碼的方式(pushTAN)，也能夠取得作為推播通知發送用來進行登入或是交易授權的 OTP。TrickMo 還包含竊取用戶設備資訊、攔截簡訊、記錄目標應用程式的一次性密碼、手機螢幕鎖定、竊取手機中圖片以及自毀和刪除機制等功能。

建議用戶自 Google Play Store 等官方商店下載 APP，避免在其他網頁或非官方應用程式安裝。下載安裝 APP 之前仔細閱讀其所要求的任何授權，避免提供 APP 需求之外的額外功能，以防止機敏資訊遭洩漏。部分惡意 APP 會偽裝成知名品牌或企業的圖示，藉此取得用戶信任並下載，用戶在安裝任何 APP 之前需先確實檢查 APP 是否為官方而非假冒的應用程式。配合廠商對於行動裝置的漏洞修補，應定期更新作業系統版本以及軟體或應用程式版本，防止遭駭客藉由漏洞竊取個資或是植入惡意軟體而造成損失。

- 資料來源：
  1. https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bank-customers-in-germany/
  2. https://www.bleepingcomputer.com/news/security/trickbot-bypasses-online-banking-2fa-protection-via-mobile-app/
  3. https://www.zdnet.com/article/trickbot-now-pushes-android-app-for-bypassing-2fa-on-banking-accounts/

## 2.2.2、香港發生 iOS 用戶遭假新聞網站駭侵事件


**資安廠商發現香港部分 iOS 用戶遭到惡意軟體攻擊，駭侵者在各網路論壇放置假冒新聞連結，誘使用戶點擊並安裝惡意軟體。**

資安廠商趨勢科技日前發表研究報告，指出該公司的資安研究人員，發現香港部分 iOS 用戶最近遭到惡意軟體攻擊；駭侵者在各網路論壇放置和假冒新聞連結，iOS 用戶一但點擊連結，就會被安裝惡意軟體。

受到攻擊的 iOS 版本，是存有某個 Safari 資安漏洞的舊版 iOS 12.1 與 iOS 12.2，如果 iOS 裝置用戶沒有更新到這些版本之後的較新版本，就有機會遭到攻擊得逞。

趨勢科技指出，誤點假冒新聞連結的用戶，會連到一個駭侵者設計的特製網站，網站中藏有三個 iFrame；用戶可見的 iFrame 會顯示正常新聞網站的內容，讓用戶誤信自己正在瀏覽正常的新聞頁面；另外有兩個用戶看不見的 iFrame，一個內含網頁統計的元件，另一個的內容就是含有惡意程式碼的網頁。

趨勢科技說，攻擊活動自二月中開始，目前仍在持續，而且就攻擊對象來看，應是針對不特定對象發動駭侵。

攻擊活動鎖定的資安漏洞，是存於 iOS 12.3、macOS Mojave 10.14.5、tvOS 12.3 和 WatchOS 5.2.1 的記憶體存取漏洞，可以用來取得 root 執行權限；接下來駭侵者就會植入一個稱為 lightSpy 的後門惡意工具，讓駭侵者可以執行任意的 shell 指令，同時存取用戶的檔案系統，同時可以竊取包括 GPS 定位、無線網路

連接記錄、硬體資料、iOS 密碼資料庫、電話通聯記錄、網頁瀏覽記錄、簡訊通聯記錄等個人資料。

- 資料來源：
  1. https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/
  2. https://www.zdnet.com/article/apple-ios-users-served-mobile-malware-in-operation-poisoned-news-campaign/

## 2.3、軟體系統資安議題

### 2.3.1、微軟 Windows 10 最新 0-day 漏洞已遭駭侵者利用


**微軟發布警告，發現有駭侵者利用最新的 Windows 10 0-day 漏洞發動攻擊，且目前尚無修補軟體可用。**

微軟發表緊急資安通報，指出在現行 Windows 10 與 Windows 7 各單機與伺服器版本中，存有兩個最新的 0-day 漏洞，可用於遠端執行任意程式碼。

這兩個 0-day 嚴重漏洞，存於 Windows 內用以處理 Adobe 字體的程式庫，駭侵者可以透過含有特製 Adobe Type 1 字體的文件檔案，誘使用戶預覽檔案，藏在文件內的惡意程式碼即可攻擊這兩個漏洞，讓駭侵者得以遠端執行任意程式碼。

微軟的聲明中說，已經觀察到利用這兩個 0-day 漏洞進行的小範圍攻擊活動，但未提供受駭者數量、攻擊來源等資訊；不過微軟也強調，攻擊活動會被局限在 AppContainer 中的沙盒內，因此駭侵者只能取得受限的系統權限與活動能力。

微軟在這份資安通報中，也詳列了所有含有這兩個 0-day 漏洞的 Windows 版本，基本上現行的 Windows 10 與 Windows 7 的單機用與伺服器版本全都入列；在報告中微軟也提供了暫時性的解決方案，包括暫時停用 Windows Explorer 中的預覽面板、停用 WebClient 服務、將 ATMFD.DLL 更名，或於登錄機碼中將其移除。

微軟目前正在趕製修補軟體，但值得注意的是，可能只有仍在支援範圍內的 Windows 10 用戶和 Windows 7 企業簽約用戶可得到支援；大批早已失去微軟支援但仍在使用中的 Windows 7 用戶，必須特別提高警覺。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv200006#ID0EMGAC
  2. https://arstechnica.com/information-technology/2020/03/attackers-exploit-windows-zeroday-that-can-execute-malicious-code/
  3. https://techcrunch.com/2020/03/23/windows-unpatched-zero-day-bug/。

## 2.3.2、微軟發表 2020 年三月 Patch Tuesday 資安修補包


**微軟發布 2020 年三月例行資安修補包，針對旗下產品的 115 個資安漏洞進行修補，建議所有微軟產品用戶即刻安裝。**

微軟每月例行發表的 Patch Tuesday 資安修補包於日前發布，繼二月修補了 99 個資安漏洞後，三月的修補漏洞數達到 115 個。

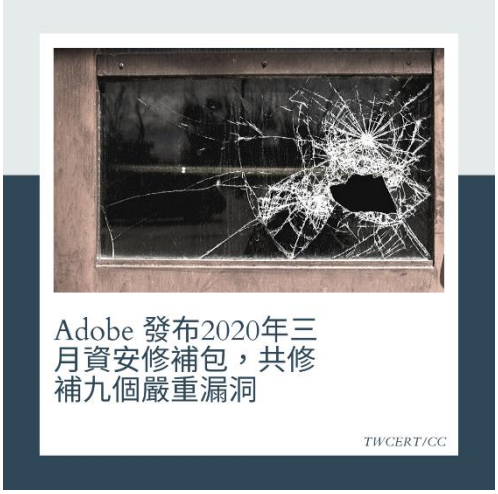
在這 115 個得到修補的資安漏洞中，其中包含 26 個可讓駭侵者遠端執行任意程式碼中的漏洞，例如 Microsoft Word 被發現的 CVE-2020-0852 漏洞，係透過特製的檔案進行駭侵；即使用戶沒有打開該檔案，還是會遭到攻擊。

再如 CVE-2020-0684 這個漏洞，駭客可利用寄送特製 .LNK 檔案給受害者，當受害者開啟後，即會被導向到含有惡意程式碼的網頁。

除微軟外，Mozilla 也推出新版 Firefox 瀏覽器，版本號碼為 74。在這個版本中，TLS 1.0 和 TLS 1.1 這兩個老舊的加密協定預設為關閉，同時針對擴充套件實施更嚴格的資安規範。在這版本中也針對 Facebook 的用戶追蹤器加入了阻擋反制機制。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Mar
  2. https://www.helpnetsecurity.com/2020/03/10/march-2020-patch-tuesday/
  3. https://www.mozilla.org/en-US/firefox/74.0/releasenotes/

## 2.3.3、Adobe 發布 2020 年三月資安修補包，修補九個嚴重漏洞




**Adobe 發布 2020 年三月資安修補包，一共修補九個嚴重漏洞，以及其他次要資安漏洞。**

Adobe 公司釋出 2020 年三月的資安修補包，修補包括 Adobe Acrobat 與 Adobe Reader 等常用軟體在內的共十三個資安漏洞。

這些本次得到修補的資安漏洞共有十三個，其中有四個屬於中等危險程度的「Important」等級，漏洞的來源樣態包括資料外洩或執行身分等級權限提升。

這四個中等程度的漏洞編號分別是 CVE-2020-3804（資料外洩）、CVE-2020-3804（資料外洩）、CVE-2020-3800（記憶體位址外洩）、CVE-2020-3083（不安全的程式庫載入導致 DLL 挾持）。

其他九個漏洞則屬於高危險的「Critical」等級；而這九個嚴重等級資安漏洞的樣態，則以遠端執行任意程式碼為主；其 CVE 編號分別為 CVE-2020-3795、CVE-2020-3799、CVE-2020-3792、CVE-2020-3793、CVE-2020-3801、CVE-2020-3802、CVE-2020-3805、CVE-2020-3807、CVE-2020-3797。

Adobe 指出，尚在使用 Acrobat DC、Acrobat Reader DC、Acrobat 2017、Acrobat Reader 2017、Acrobat 2015、Acrobat Reader 2015 的 Windows 與 MacOS 用戶，請盡快升級到最新版本，以修補上述資安漏洞。

Adobe 公司經常在微軟發表 Patch Tuesday 每月資安修補包時，同步推出自己的當月資安修補包。

- 資料來源：
  1. https://helpx.adobe.com/security/products/acrobat/apsb20-13.html
  2. https://www.bleepingcomputer.com/news/security/adobe-fixes-nine-critical-vulnerabilities-in-reader-acrobat/

## 2.3.4、以色列行銷業者未正確保護資料庫，Email 等多項個資在網上曝光


**以色列數位行銷業者未能妥善處理系統資安設定，導致近五千萬人的電子郵件信箱等個資在網路曝光。**

據媒體報導指出，這家名為 Straffic 的以色列數位行銷公司外洩的資料庫大小，高達 140GB，內含個資除了 Email 外，還包括姓名、電話號碼、實體地址等。

這個資料庫存放在 AWS 上，可能是因為 Straffic 的人員未能正確設定伺服器與資料庫的資安原則，同時沒有適當存放其登入資訊，導致這起外洩事故。

獨立資安研究者在研究垃圾信件寄送過程時，無意發現了存在網路上的某個 .env 檔，內含指向某個 Elasticsearch 資料庫的登入資訊，該研究者因而發現這個巨大資料庫。

該公司於二月 26 日發表簡短聲明，承認發生資料外洩事件，但強調問題已經解決，且尚未發現這批資料有遭濫用或被竊的情形。

著名資安研究者 Troy Hunt 指出，這批曝光的 Email 地址當中，已經有七成都在他提供的「Have I been Pwned」被駭資料庫中出現，但這也表示有多達三成的 Email 是過去未曾被竊過的。

- 資料來源：
  1. https://www.bankinfosecurity.com/israeli-marketing-company-exposes-contacts-database-a-13785
  2. https://www.bleepingcomputer.com/news/security/49-million-unique-emails-exposed-due-to-mishandled-credentials/
  3. https://straffic.io/updates.php

## 2.3.5、國內與美國網通大廠路由器遭駭，用戶會被誤導下載惡意軟體


**資安廠商發現新型駭侵手法，駭侵者駭入國內與美國網通大廠家用路由器，竄改 DNS 設定，以提供 COVID-19(新冠肺炎、武漢肺炎)資訊為由，誘使用戶下載惡意軟體。**

資安廠商 Bitdefender 的研究團隊發表最新報告指出，該公司發現新型駭侵手法；駭侵者駭入國內與美國網通大廠家用路由器，竄改 DNS 設定，將用戶的部分網路連線重新導向至不明網站，並以提供 COVID-19 資訊為由，誘使用戶下載惡意軟體。

據 Bitdefender 的報告，這波駭侵攻擊首先以暴力嘗試法，試圖找出家用路由器的管理者帳密，登入成功後會進入 web 管理界面，將 DNS 伺服器設定更改為 109.234.35.230 與 94.103.82.249，接下來利用這兩台假的 DNS 伺服器，將部分特定網路瀏覽流量導向至存有惡意軟體 Bitbucket 的網站。

為了防止用戶發現網址有異，駭侵者也利用 TinyURL 縮址服務，隱藏 Bitbucket 的真實網址，等用戶按下下載按鈕後，即讓用戶安裝 Oski 資訊竊取惡意軟體。

會被劫持至惡意網站的 URL，包括 aws.amazon.com、gog.gl、bit.ly、disney.com、pubads.g.doubleclick.net 等，含蓋一般用戶常去的網站，或是網頁元件的常用 hosting 網址等。

據 Bitdefender 表示，一星期以來約觀測到千餘起攻擊事件；建議路由器用戶，請務必檢視自己路由器的 DNS 設定，如果發現被改為上述 IP，請立即更正。

- 資料來源：
  1. https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/
  2. https://www.bleepingcomputer.com/news/security/hackers-hijack-routers-dns-to-spread-malicious-covid-19-apps/
  3. https://www.zdnet.com/article/d-link-and-linksys-routers-hacked-to-point-users-to-coronavirus-themed-malware/

## 2.3.6、百萬台 Toyota、Hyundai、KIA 汽車面臨無線車鑰遭駭侵者複製風險


**資安專家指出 Toyota、Hyundai、KIA 等三家車廠使用的無線車鑰系統，其加密演算法存有資安漏洞，駭侵者可輕易取得密鑰資訊，進而竊走車輛。**

比利時 KU Leuven 大學和英國伯明罕大學的研究人員，日前共同發表研究報告，指出市售多款 Toyota、Hyundai、KIA 車輛使用的無線車鑰加密傳輸協定，存有嚴重漏洞，其加密密鑰可被駭侵者輕易複製。

該研究報告指出，這三大車廠的部分車款，其無線車鑰系統使用的德州儀器 DST80 系統，存有資安漏洞；駭侵者可以利用售價相當便宜的 RFID 掃瞄傳輸裝置，在一定距離內掃瞄無線車鑰，就能取得足夠的資訊；接下來還可以用同一個 RFID 掃瞄傳輸裝置偽裝成真正的無線車鑰，開啟車門並發動車輛。

受該漏洞影響的車款，包括 Toyota 2008 年到 2016 年的 Auris、Camry、Corolla、RAV 4、Yaris、Hiace、Hilux 等，KIA 2011 到 2017 年的 Carens、Soul、Picanto 等，以及 Hyundai 2008 到 2013 年的 i10、i20、IX20、Veloster 等車款。

據 Wired 報導指出，Toyota 已經確認這個資安漏洞確實存在，但該公司認為實務上並不容易使用這個漏洞來竊取車輛，因為必須在很短的距離內才能進行無線車鑰的掃瞄。

值得注意的是，該報告也列入了 Tesla Model S 2018 年款式，不過 Tesla 在去年發布的韌體更新中，已經修補了這個漏洞。

詳細的車款列表，可參考表 1 受影響車輛列表。

表 1、受影響車輛列表

| Make | Period | Model |
|---|---|---|
| Toyota | 2009-2013 | **Auris (2011)** |
| | 2010-2013 | Camry |
| | 2010-2014 | Corolla |
| | 2011-2016 | FJ Cruiser |
| | 2009-2015 | Fortuner |
| | 2010+ | Hiace |
| | 2008-2013 | Highlander |
| | 2009-2015 | **Hilux (2014)** |
| | 2009-2015 | Land Cruiser |
| | 2011-2012 | RAV4 |
| | 2010-2014 | Urban Cruiser |
| | 2011-2013 | Yaris |
| Tesla | 06/2018-07/2019[1] | **Model S (2018)** |

| Make | Period | Model |
|---|---|---|
| Kia | 2012+ | **Ceed (2016)** |
| | 2014 | **Carens (2014)** |
| | 2011-2017 | Rio |
| | 2013+ | Soul |
| | 2013-2015 | Optima |
| | 2011+ | Picanto |
| Hyundai | 2008+ | I10 |
| | 2009+ | I20 |
| | 2009+ | I20 |
| | 2010+ | Veloster |
| | 2016 | **IX20 (2016)** |
| | 2013 | **I40 (2013)** |

資料來源：UNIVERSITY OF BIRMINGHAM AND KU LEUVEN

- 建議採取資安強化措施

1、建議受影響車輛列表的車主，應至廠商官網查詢車輛的最新資安漏洞訊息，或是與原車廠進行聯繫，保障車輛安全。

2、車主應根據車廠釋出的新版韌體，將韌體更新至最新版本，以修補漏洞，避免車子遭竊。

- 資料來源：

1. https://tches.iacr.org/index.php/TCHES/article/view/8546/8111
2. https://www.wired.com/story/hackers-can-clone-millions-of-toyota-hyundai-kia-keys/

# 2.4、軟硬體漏洞資訊

## 2.4.1、Microsoft Exchange 伺服器存有資安漏洞，建議立即更新至最新版本


**Microsoft Exchange 伺服器被發現 CVE-2020-0688 的資安漏洞。**

這個漏洞是 Exchange 伺服器未能在安裝時產生唯一的金鑰，導致駭客能以系統權限傳遞任意物件，進行遠端程式攻擊。該漏洞存在於 Exchange 控制面板元件中，使用靜態金鑰為 ViewState 提供安全性，而不是在安裝時隨機產生金鑰，並且所有 Exchange 伺服器的 web.config 都存有相同的驗證與解密金鑰。經過身分驗證的駭客能以系統權限的方式，在 Exchange 伺服器執行任意程式碼，並破壞目標伺服器。

Microsoft 已在二月的 Patch Tuesday 修補此漏洞，呼籲用戶應立即更新至最新版本，盡速完成 Exchange 漏洞修補，以免造成損失。

- CVE 編號：CVE-2020-0688
- 影響版本： Microsoft Exchange Server 2010、2013、2016、2019
- 解決方案：立即將 Exchange 更新至最新版本，檢視 IIS 與 Exchange 相關紀錄，釐清是否存有異常連線或檔案下載/執行等，以確認是否被利用漏洞入侵疑慮。

- 資料來源：
  1. https://www.thezdi.com/blog/2020/2/24/cve-2020-0688-remote-code-execution-on-microsoft-exchange-server-through-fixed-cryptographic-keys
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688
  3. http://tacert.tanet.edu.tw/prog/shownews.php?id=3003

## 2.4.2、使用國內企業晶片的 Android 手機出現嚴重資安漏洞


**廣泛用於中低階 Android 手機的國內某企業 64 位元處理器，日前被發現存有嚴重資安漏洞，用簡單的指令即可取得 root 權限。**

這個 CVSS 嚴重程度評分高達 9.3 分的極嚴重漏洞，在 2019 年就於 XDA-Developer 上被獨立資安研究人員提出，並將之命名為「MediaTek-SU」。

該研究人員是在試圖破解自己的 Amazon Fire 平板電腦時，發現這個嚴重的漏洞；只要用幾行指令，連 bootloader 都不需要，就可以立即取得系統最高的 root 權限，幾乎可以為所欲為。

據 XDA-Developers 網站上的資料，下列該企業的晶片都存有這個嚴重的漏洞：MT6735、MT6737、MT6738、MT6739、MT6750、MT6753、MT6755、MT6757、MT6758、MT6761、MT6762 、MT6763、MT6765、MT6771、MT6779、MT6795、MT6797、MT6799、MT8163、MT8167、MT8173、MT8176、MT8183、MT6580 和 MT6595；以品牌來看則至少包括 Vivo、華為、榮耀、Oppo、三星等，系統版本則為 Android 7、8、9。

雖然在去年就修補了這個漏洞，新版的 Android 10 也已不受影響，但由於處理器多半用在中低階 Android 裝置，生產這類中低階裝置的廠商，多半不會在產品上市後積極提供系統軟體更新服務，因此市面上恐有大量 Android 裝置存有這個漏洞，而且難以全面修補。

- CVE 編號：CVE-2020-0069
- 影響產品：採用國內某企業處理器的 Android 7、8、9 裝置
- 資料來源：
  1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0069
  2. https://forum.xda-developers.com/android/development/amazing-temp-root-mediatek-armv8-t3922213
  3. https://www.xda-developers.com/mediatek-su-rootkit-exploit/

## 2.4.3、協作通訊平台 Slack 被發現重大漏洞，可能導致大量帳號遭盜


**獨立資安研究人員 Evan Custodio 在資安通報平台 Hackerone 上，發表一個 Slack 的嚴重漏洞；該漏洞可能導致大量用戶資料外洩，甚至帳號被駭侵者盜走。**

Custodio 在漏洞報告中指出，這個漏洞是利用所謂「HTTP 請求走私」，駭侵者可利用這個漏洞進行以 CL.TE 為基礎的封包挾持，並且竊得用戶階段的私密 cookie；受害者的 Slack 通訊將會被重新導向到駭侵者指定的 client。

透過這種攻擊手法，駭侵者即可取得 Slack 受害用戶的各種資料，並透過自動化的方式，大量取得眾多 Slack 用戶的帳號存取權，是非常嚴重的漏洞。

這個漏洞的 CVSS 危險程度評分高度 9.3 分。

該漏洞是在去年 11 月就透過 Hackerone 平台提報給 Slack，Slack 也很快的在 24 小時內修補該漏洞；漏洞相關情報在近日才予以公開。

- 影響產品：Slack

- 資料來源：
  1. https://hackerone.com/reports/737140
  2. https://www.zdnet.com/article/slack-vulnerability-allowed-session-hijacking-account-takeovers/

## 2.4.4、近年出品之 Intel 處理器，內含難以修復的資安漏洞


**資安廠商 Positive Technologies 上周發表研究報告，指出近年出品的 Intel 各型 x86 處理器，內含無法修復的資安漏洞，恐將造成大規模針對此漏洞的駭侵攻擊。**

這個漏洞之所以無法修復，是因為該漏洞存在於處理器的 ROM 區塊；該區塊中一個稱為 Intel Coveraged Security Management Engine (CSME) 的重要區塊出現程式漏洞，而這個區域的程式碼是寫死（Hard coded）在硬體中的，因此難以更動。

CSME 是 x86 電腦系統中最低階的資安驗證系統，但因為該漏洞的存在，駭侵者可以透過特殊設計的程式碼來欺騙 CSME 中的驗證程序，導致整台電腦的所有安全驗證體系，包括儲存資料的加密、DRM、硬體的加密數位簽章等都將因此失效；攻擊者甚至可以透過該漏洞，在極低階的硬體上直接執行任意程式碼，所有軟體的防毒防駭機制均無法偵測。

Intel 雖然早在 2019 年初就知道這個漏洞的存在，也已發表修補程式，但據 Positive Technologies 的報告指出，這個修補程式只從一個方向阻擋利用此漏洞的駭侵攻擊，仍有相當多方法可以利用此漏洞進行駭侵攻擊。

根據 Intel 的資安通報，這個漏洞的 CVSS 危險程度評級達 7.1 分，屬高危險等級。

- CVE 編號：CVE-2019-0090

- 影響版本：Intel CSME 12.0.35 之前版本

- 資料來源：
  1. https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00213.html
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0090
  3. http://blog.ptsecurity.com/2020/03/intelx86-root-of-trust-loss-of-trust.html
  4. https://www.theverge.com/2020/3/6/21167782/intel-processor-flaw-root-of-trust-csme-security-vulnerability

## 2.4.5、Netgear 部份路由器產品新發現多個嚴重資安漏洞


**無線網路設備大廠 Netgear 日前發布資安通報，指出旗下多款路由器產品發現存有多個資安漏洞，包括 2 個高度危險漏洞、21 個中度危險漏洞、1 個低度危險漏洞。**

其中最危險的 2 個安全漏洞，都發生在 Nighthawk X4S Smart Wi-Fi Router（R7800）產品，其中一個 CVSS 評分高達 9.4 分，發生在韌體版本 1.0.2.68 之前，可讓駭侵攻擊者取得整台路由器的控制權；另一個 CVSS 高達 8 分的漏洞，發生在韌體版本 1.0.2.60 之前，可讓攻擊者注入指令，並可因此取得 root 控制權限。

這個可注入指令的資安漏洞，同樣也出現在 Netgear 另外 29 款路由器產品，分別是 D6000, R6000, R7000, R8000, R9000 和 XR500 系列產品。

除了上面提到的兩個資安漏洞外，稍早 Netgear 也曾針對其 R6400、R6700、R6900、R7900 系列產品發布資安通報，指出某些版本的韌體也含有高危險資安漏洞，同樣也是可讓駭侵者注入指令的漏洞。

Netgear 在資安通報中提供了更新修補檔案與教學，建議擁有上述機種設備的用戶，盡快更新到最新版韌體，以修補這些嚴重的資安漏洞。

- 影響產品(版本)：

  Nighthawk X4S Smart Wi-Fi Router（R7800）韌體版本 1.0.2.68 之前

  Nighthawk X4S Smart Wi-Fi Router（R7800）韌體版本 1.0.2.60 之前

  D6000, R6000, R7000, R8000, R9000 和 XR500 系列產品

  R6400、R6700、R6900、R7900 系列產品

- 解決方案：升級到最新版本韌體

- 資料來源：

  1. https://kb.netgear.com/000061741/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-Routers-PSV-2019-0051
  2. https://kb.netgear.com/000061760/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-Routers-and-Gateways-PSV-2018-0352
  3. https://kb.netgear.com/000061740/Security-Advisory-for-Unauthenticated-Remote-Code-Execution-on-R7800-PSV-2019-0076
  4. https://threatpost.com/critical-netgear-bug-impacts-nighthawk-router/153445/

## 2.4.6、開源路由器韌體 OpenWrt 修正遠端執行漏洞


**廣受喜愛，基於 Linux 的開放源碼路由器韌體 OpenWrt，日前修復一個可用於遠端執行任意程式碼的嚴重資安漏洞。**

這個資安漏洞編號為 CVE-2020-7982，問題出在 OpenWrt 處理程式套件包裝 opkg 檔案時，未事先對下載回來的 .ipk 檔案進行必要的資安檢查；這個錯誤可讓駭侵者透過特意撰寫並置入惡意軟體的 ipk 檔案，取得路由器的 root 權限；不但可存取整個檔案系統，當然也能執行任意程式碼。

不過，駭侵者必須先在路由器下載程式套件的 OpenWrt 官方網站與攻擊目標的路由器間進行中間人攻擊，透過未加密的 http 連線，傳送合法且經過簽署的惡意程式套件給被攻擊目標路由器。

發現此漏洞的資安專家 Fuido Vranken 指出，駭侵者可以先以 DNS 挾持的方式，將原本要連向 OpenWrt 官方下載網站的連線，誤導到含有惡意軟體的網站，即可大幅簡化攻擊流程。

這個 CVE-2020-7982 的嚴重程度分數為 8.1 分，嚴重程度評級為「高」。

受此漏洞影響的 OpenWrt 版本，從 18.06.6 到 19.07.0 之前的各版本，更新版已在 2020 年 2 月 1 日推出；用戶如果在自己的路由器上安裝過舊版 OpenWrt，應依照 OpenWrt 組織的建議，立即更新至最新版本，以加強資安防護。

- CVE 編號：CVE-2020-7982

- 影響版本：18.06.6、19.07.0 之前版本

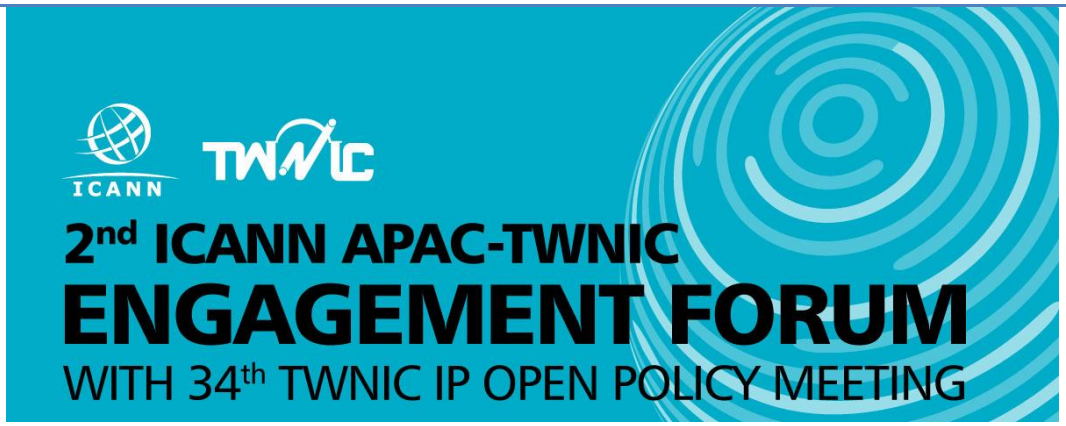
- 解決方案：升級至最新版本韌體

- 資料來源：
  1. https://openwrt.org/advisory/2020-01-31-1
  2. https://nvd.nist.gov/vuln/detail/CVE-2020-7982
  3. https://www.securityweek.com/remote-code-execution-vulnerability-patched-openwrt

# 第 3 章、 資安研討會及活動

| 第 19 屆亞太資訊安全論壇暨展會 | |
|---|---|
| **活動時間** | **6/9 (二) – 6/10 (三) 09:00 ~ 17:00** |
| **活動地點** | **台北市敦化南路一段 108 號 B2F** |
| **活動網站** | **https://www.informationsecurity.com.tw/event/event_info.aspx?eid=1498** |
| **活動概要** |  <br>參加對象: 政府、金融、醫院、高科技製造業等產業資安、網管、IT、程式等人員 。<br>參加方式: 全程免費參加 / 報名請務必留下公司 email 及電話。<br>同期展出: 政府論壇、關鍵資訊基礎、金融論壇、製造業論壇、醫療論壇等專屬研討會。<br>參加提醒: 請務必攜帶任職公司的個人職務名片前來報到換取會議入場證。<br>注意事項: 主辦單位享有審核參與人員之權力，同時本活動因須審核產業屬性，恕不接受現場報名。<br><br>活動洽詢: 02-8729-1042 潘小姐 / Iris.Pan@newera.messefrankfurt.com<br>主辦單位: 資安人 |

| CYBERSEC 2020 臺灣資安大會 | |
|---|---|
| **活動時間** | **8/12(二) – 8/14(四) 08:30 ~ 17:00** |
| **活動地點** | **台北市南港區經貿二路 2 號 (南港展覽二館)** |
| **活動網站** | https://r.itho.me/sec2020 |
| **活動概要** |  <br>國際級資安大會 X 超規格資安大展【CYBERSEC 2020 臺灣資安大會】，即將在 8/12-8/14 於南港展覽二館盛大登場！<br><br>匯聚世界級資安大神、國內資安頂尖高手，從提供超過 200 堂資安面向的議程、量身打造最扎實的 CyberLab 實戰演練課程，探討國際最新、最熱門且最全面的資安議題與技術，讓您全方面迎戰資安風險。即刻提升實戰能力。<br><br>現場網羅超過 250 家以上全球與國內知名標竿資安品牌，展示 1000+業界最新、最適切的資安產品與服務。平日難以跟進的所有資安產品資訊、市場與發展，都可以在此一次獲得！<br><br>邀請您與我們一同參與這年度資安盛會，與來自臺灣與亞太地區超過 8,000 位菁英進行交流，從技術層面與策略層面，探討資安百種面向、交流技術與知識，讓資安戰場更加壯大，得以更快速地反應、更快速地處理，形成足以跟攻擊者匹敵的更強力防禦。<br>主辦單位：iThome<br>了解更多大會資訊：https://r.itho.me/sec2020 |

| 第二屆 ICANN APAC-TWNIC Engagement Forum 與第 34 屆 TWNIC IP 政策資源管理會議 | |
|---|---|
| **活動時間** | **2020 年 11 月 12、13 日** |
| **活動地點** | **台北市仁愛路三段 160 號** |
| **活動網站** | **https://forum.twnic.tw/2020/registration.htm** |
| **活動概要** |  <br>網際網路名稱與數字位址分配機構（ICANN）及財團法人台灣網路資訊中心（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。<br><br>第 34 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。<br><br>本次論壇邀請喬治亞科技大學公共政策學院的 Milton Mueller 教授擔任專題演講主講人，他的主要研究領域為網路的政經發展，主題涵蓋網路所有權、運作機制及資通訊產業的全球治理。他是網路治理計畫的創立者之一，在 ICANN 及 OECD 的公民社群中具有領導地位。曾經參與建立非商業使用者選舉人並當選兩次主席、擔任 GNSO 議會委員；並於多個 ICANN 工作小組中服務，曾擔任 PIR(.org)之諮詢議會委員。參與網路治理經驗豐富，演講內容精彩可期。 |

| | |
|---|---|
| | 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。 |

# 第 4 章、 2020 年 03 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。

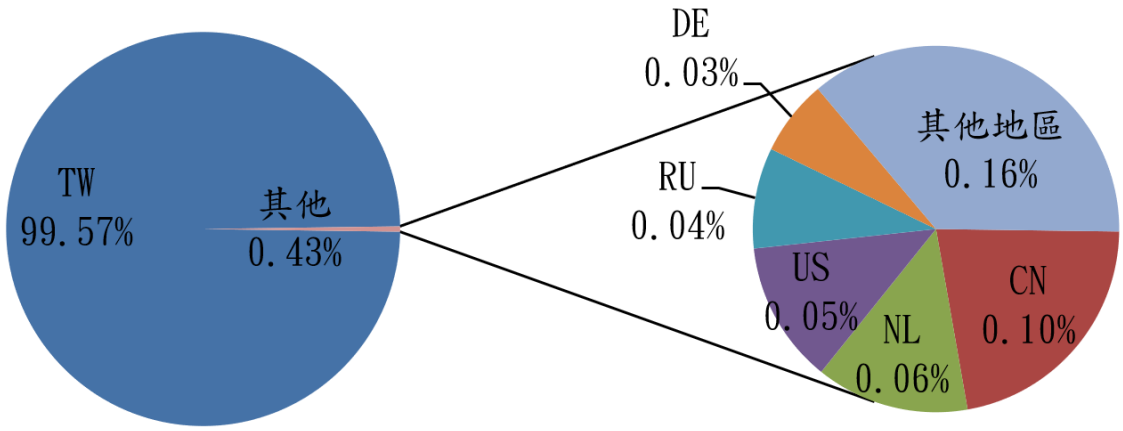



圖 1、分享地區統計圖

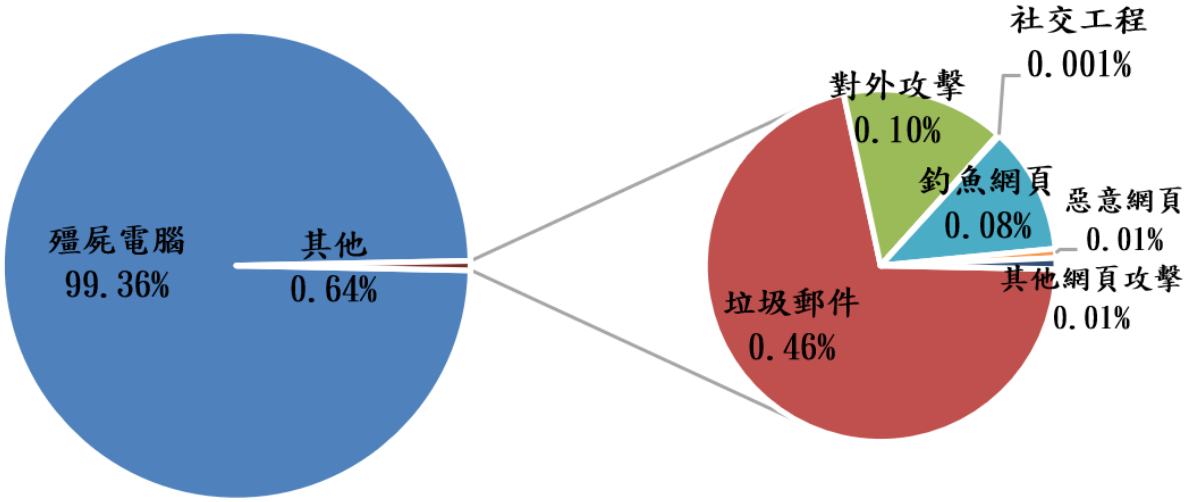

殭屍電腦
99.36%
其他
0.64%
社交工程
0.001%
對外攻擊
0.10%
釣魚網頁
0.08%
惡意網頁
0.01%
其他網頁攻擊
0.01%
垃圾郵件
0.46%

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：**2020 年 4 月 10 日**

編輯：**林克容、江奕昉、洪彩馨**

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**