



TWCERT/CC 資安情資電子報

TWCERT/CC 資安情資電子報

2024 年 6 月份

2024 年 6 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：本月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。範疇可能包含資安趨勢、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、軟硬體系統資安議題、軟硬體漏洞資訊及新興應用資安。

第3章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第4章、TVN漏洞公告：TWCERT/CC為CVE編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明本月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN)平台其CVSS 3分數為8.8以上之漏洞。

目錄

內容

目錄 II

第 1 章、封面故事.....	1
PHP 存在遠端程式碼執行漏洞(CVE-2024-4577) · 官方緊急發布修補版本	1
第 2 章、國內外重要資安事件.....	3
2.1 新興應用資安.....	3
2.1.1 針對 AI 語音生成工具的新型惡意程式 Gipy	3
2.2 國際政府組織資安資訊.....	5
2.2.1 2024年巴黎奧運之網路威脅探討	5
2.3 軟硬體系統資安議題.....	9
2.3.1 Github 成為網路勒索攻擊目標 · 駭客盜用帳號Gitloker 進行攻擊.....	9
2.3.2 Phoenix UEFI 漏洞影響多款 Intel CPU 設備	12
2.4 軟硬體漏洞資訊.....	14
2.4.1 Check Point VPN Gateway存在高風險安全漏洞	14
2.5.2 PHP存在高風險安全漏洞.....	15
2.5.3 以Chromium為基礎之瀏覽器存在安全漏洞	17
第 3 章、資安研討會及活動	19
第 4 章、TVN 漏洞公告.....	31
編輯：TWCERT/CC 團隊.....	37

第 1 章、封面故事

PHP 存在遠端程式碼執行漏洞(CVE-2024-4577)，官方緊急發布修補版本



資安業者戴夫寇爾研究團隊發現PHP存在引數注入(Argument Injection)漏洞(CVE-2024-4577)，可在遠端伺服器上執行任意程式碼並通報給 PHP 官方。PHP 在網站開發中應用廣泛，官方已於 2024年6月6日在網站上發佈修補版本，建議使用者儘速更新。

此漏洞源於 PHP 設計未注意到 Windows 作業系統字元編碼轉換的Best-Fit 特性，使得未經身分鑑別之遠端攻擊者可透過特定字元序列繞過CVE-2012-1823之保護，並透過引數注入(Argument Injection)等攻擊，於遠端PHP伺服器上執行任意程式碼。

此漏洞影響所有安裝在 Windows 作業系統上的 PHP 版本，包括：

- PHP 8.3 版本低於 8.3.8

- PHP 8.2 版本低於 8.2.20
- PHP 8.1 版本低於 8.1.29

另因PHP 8.0 分支、PHP 7 以及 PHP 5 官方已不再維護，建議使用這些版本的網站管理員更換成PHP官方仍有維護之版本，或採取相應的緩解措施。

若需確認網站是否受影響，管理員可以檢查 Apache HTTP Server 的設定，當網站設定在CGI 模式下執行PHP或將 PHP 執行檔暴露在外時，該伺服器將容易成為攻擊的目標。需特別注意的是，若使用 XAMPP for Windows 預設安裝配置，也會受此漏洞影響。

研究團隊指出，當 Windows 作業系統設置為繁體中文、簡體中文或日文語系時，未經授權的攻擊者可以直接在遠端伺服器上執行任意程式碼。雖然其他語系的 Windows 系統也可能存在風險，但具體影響範圍仍需使用者自行檢查並盡早更新 PHP 版本。

PHP 官方目前已發布最新版本(8.3.8、8.2.20 和 8.1.29)來修復此漏洞，強烈建議所有使用者立即升級至最新版本，以確保系統安全。對於無法升級的系統，管理員可以考慮其他暫時緩解措施，如修改 Rewrite 規則以阻擋攻擊或取消 PHP CGI的功能。

此外，PHP CGI 已被認為是一種過時且易受攻擊的架構，建議使用者評估並遷移至更為安全的 Mod-PHP、FastCGI 或 PHP-FPM 等架構。

- 資料來源：
 1. [官方網站更新資訊](#)
 2. [\[DEVCORE\]資安通報: PHP 遠端程式碼執行 \(CVE-2024-4577\) - PHP CGI 參數注入弱點](#)

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 針對 AI 語音生成工具的新型惡意程式 Gipy



卡巴斯基研究人員發現新型惡意程式並命名為 Gipy，此惡意程式通過釣魚網站提供 AI 語音應用程式來感染使用者電腦，進行資料竊取和安裝其他惡意程式，研究人員發現攻擊多數來自透過 WordPress 架設的網站，並從 Github 下載受密碼保護的 zip 檔案解壓出惡意程式，主要受害地區包括德國、俄羅斯、西班牙和台灣。

隨著 AI 工具普及，更多攻擊者利用這些工具進行惡意活動，顯示犯罪市場對資料竊取工具的需求增加。卡巴斯基在近期的攻擊活動中觀察到，攻擊者會架設釣魚網站，內容是提供 AI 語音相關應用程式，當使用者從這些網站下載並執行就會中毒，而目前觀察到多數都是透過 WordPress 架設起來。

卡巴斯基研究人員指出，Gipy 惡意程式最早出現於 2023 年，當

惡意程式被成功植入，可以竊取使用者電腦資料，並在受害者電腦上安裝其他惡意程式，當使用者執行下載的程式，會正常的執行AI語音相關應程式，並在使用者電腦後台隱性的執行 Gipy 惡意程式，受害者不容易發現。

研究人員發現當 Gipy 惡意程式執行的時候，會從 Github 啟動受密碼保護的 zip 檔案，從中解壓縮出惡意程式，在整個研究的過程中，卡巴斯基研究員目前分析到了 200 多個檔案，並在一封電子郵件裡對這些分析的檔案做一個整理：

- 資料竊取工具：Lumma、RedLine、RisePro 和 LOLI Stealer
- 虛擬貨幣挖擴程式：Apocalypse ClipBanker
- 木馬程式：DCRat 和 RADXRat
- 後門程式：TrueClient

卡巴斯基研究員表示隨著人工智慧工具的普及，越來越多攻擊者利用人工智慧工具作誘餌來進行惡意威脅活動，Gipy 惡意程式並無特別針對哪個目標國家進行攻擊，但目前最主要受影響的前 4 大地區有德國、俄羅斯、西班牙、台灣。

卡巴斯基針對從網路下載檔案，提出相關的安全建議：

- 下載軟體務必從官網下載，而不是其他第三方平台下載
 - 務必驗證網站的合法性，確保網址是 https 開頭，且憑證是合法的而非自簽憑證或過期的憑證
 - 使用者電腦的帳號密碼務必啟用雙重驗證，並為每個帳戶使用獨立的密碼
 - 警惕任何未知來源的電子郵件和可疑連結
- 資料來源：
 1. [AI Voice Generator App Used to Drop Gipy Malware](#)

2.2 國際政府組織資安資訊

2.2.1 2024年巴黎奧運之網路威脅探討



Mandiant 研究人員指出，俄羅斯贊助的國際 APT 組織對於 2024 年巴黎奧運可能造成高度威脅。威脅源自法國親烏克蘭的立場，以及俄羅斯無法正式參加奧運會的政治報復。相比之下，與中國、伊朗和北韓有關的 APT 組織對奧運構成的網路威脅相對較低。

Mandiant 列出了與奧運賽事相關的 APT 組織，分別是中國的 APT 15、APT 31、UNC 4713、Temp.Hex，北韓的 APT 43，俄羅斯的 APT 28、APT 44、UNC 4057，伊朗的 APT 42，以及白俄羅斯的 UNC 1151。這些組織針對奧運的網路威脅和潛在目標主要是政治因素或經濟利益驅動。從政治角度來看，網路釣魚可能以運動賽事為誘餌，達到特定的政治目的。而從經濟角度來看，這些攻擊可能涉及門票詐騙、攻擊 POS 機器、勒索軟體攻擊，以及竊取運動員個人資料並在暗網販售等。

俄羅斯可能造成的網路威脅

俄羅斯攻擊的因素主要有兩個，一是俄羅斯運動員今年可以參賽，但僅能以中立運動員身份參加，無法代表祖國，這引起了俄羅斯的不滿。二是法國在 2022 年俄羅斯入侵烏克蘭後提供了相關的軍事支持，這可能引發俄羅斯的報復行動。鑒於此，Mandiant 推測俄羅斯的 APT 組織對 2024 年巴黎奧運可能會造成相當的威脅。

過去的案例，這些 APT 組織也有針對奧運進行相關的網路威脅活動，例如：

- 英國國家網路安全中心 (NCSC) 觀察到 APT 44 針對 2020 年東京奧運的攻擊證據
- Mandiant 指出 APT 44 在 2018 年冬季奧運期間使用惡意程式 (Olympic Destroyer) 中斷奧運賽事開幕期間網路服務
- Google 威脅分析小組 (TAG) 發現 APT 44 在 2017 年底針對 2018 年冬季奧運進行攻擊，利用 Play 商店散播 CHEMISTGAMES 惡意程式
- 美國司法部在 2018 年指控 APT 28 攻擊 2016 年巴西奧運，並向反興奮劑組織發送釣魚信件
- Mandiant 觀察到 APT 28 在 2016 年巴西奧運後洩漏運動員資料

中國及伊朗可能造成的網路威脅

針對中國的威脅，Mandiant 指出中國支持的 APT 組織長期以來對歐洲政府和企業進行攻擊，因此，也可能會影響 2024 年奧運。這些威脅主要以網路釣魚和情報收集為主。過去針對歐洲的中國 APT 組織包括 APT 31、APT 15、UNC 4713 及 TEMP.Hex，其中網路威脅事件包括：英國指出 APT 31 在 2021 年探查英國議員的電子郵件帳號；UNC 4713 針對多國進行釣魚攻擊，意圖在 G7 高峰會傳播

EIGHTFLY 惡意程式；TEMP.Hex 自 2023 年 4 月起對歐洲政府進行網路釣魚攻擊。

Mandiant 指出，伊朗贊助的 APT 42 組織過去一直針對歐洲進行間諜活動，近期的加薩衝突可能會影響其網路間諜行動。

奧運期間遭受的攻擊

在過去的歷史事件中，2021 年東京奧運和 2018 年冬季奧運均遭受多次網路攻擊。

- 2021 年東京奧運
 - 北韓的 APT 組織利用東京奧運為誘餌進行網路釣魚，投放惡意程式 CABRIDE 和 CABSERVICE
 - 世界反興奮劑組織 (World Anti-Doping Agency , WADA) 於 2019 年發現俄羅斯運動員藥檢結果有問題，導致俄羅斯被禁賽，進而引發俄羅斯政府支持的 APT 28 對反興奮劑機構的攻擊
 - 日本奧委會指出其網路在 2020 年 4 月被一個不知名的勒索軟體攻擊，導致其組織運作暫時停止
- 2018 年冬季奧運
 - 開幕期間官網遭受攻擊，造成網站中斷 12 小時，使得使用者無法列印門票和存取賽事資訊。Mandiant 認為這可能是由 Sandworm Team 駭客組織所為
 - 出現利用韓語的奧運參賽程式作為誘餌，誘導使用者下載惡意程式 GARPUN
 - APT 28 組織註冊一組專門欺騙運動相關組織的網域名稱
 - Fancy Bears 駭客組織洩漏屬於國際奧林匹克委員會官員的信件

針對這些威脅，Mandiant建議參與賽事的相關單位應加強資安宣導和社交工程培訓，且參加賽事的使用者建議使用一次性設備，不隨意連接不認識的 WiFi，並避免遠端存取敏感資料；參加賽事期間盡量不要遠端存取敏感資料，帶出去的設備盡量不要存有敏感個資。透過相關安全措施，以減少網路安全威脅對所帶來的潛在風險。

● 資料來源：

1. <https://www.cna.com.tw/news/aopl/202406040256.aspx>
2. <https://today.line.me/tw/v2/article/MVewNa>
3. <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>
4. <https://www.mandiant.com/sites/default/files/2022-03/wp-ddos-protection-recommendations.pdf>
5. <https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm>
6. <https://cyberscoop.com/fancy-bear-olympics-hacking-tokyo/>
7. <https://www.mandiant.com/sites/default/files/2022-06/wp-proactive-prep-and-hardening-wp.pdf>
8. https://www.lemonde.fr/en/international/article/2024/03/22/insults-provocations-cyberattacks-russia-scales-up-hostility-toward-france_6644718_4.html
9. <https://apnews.com/article/paris-olympics-ioc-russia-e08f47312dc558eb885825ed0f8874ee#:~:text=Russia and Belarus are barred,to be granted neutral status.>
10. <https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games>
11. <https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf>
12. <https://www.theguardian.com/sport/2018/feb/11/winter-olympics-was-hit-by-cyber-attack-officials-confirm>
13. <https://www.nytimes.com/2019/09/23/sports/olympics/russia-doping-wada.html>
14. https://www.lemonde.fr/en/sports/article/2024/04/10/paris-2024-new-tickets-to-be-released_6668021_9.html

2.3 軟硬體系統資安議題

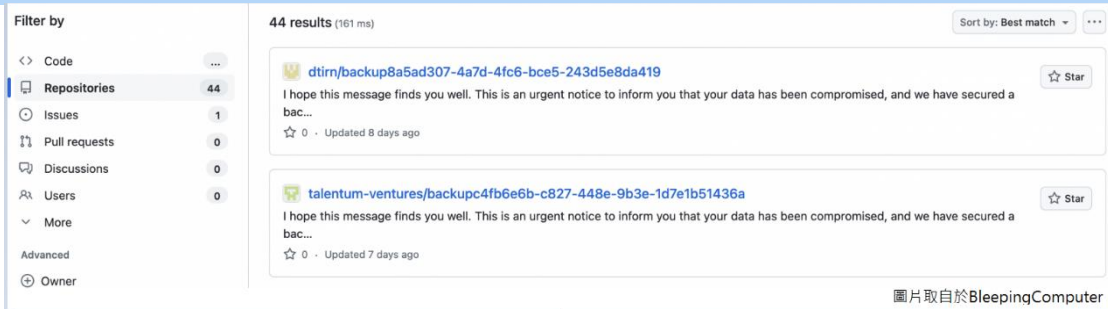
2.3.1 Github 成為網路勒索攻擊目標，駭客盜用帳號Gitloker 進行攻擊



智利資安公司 CronUp 研究人員 German Fernandez 發現駭客攻擊 Github 專案儲存庫，駭客疑似竊取使用者憑證進行攻擊活動，此次攻擊即是利用 Telegram 中的 Gitloker 帳號，偽造為資安分析師進行釣魚行為。

German Fernandez 指出，今年從 2 月開始，一直有駭客透過竊取或刪除他人的 Github 專案儲存庫來勒索受害者。

攻擊者竊取受害者的專案儲存庫之後，重新命名專案儲存庫，並添加一個檔案：README[.]me，告知受害者可透過 Telegram 聯繫攻擊者，其勒索信內容為：「這是一個緊急通知，你的資料已經外洩，我們有幫你備份好資料並確保其安全」。



German Fernandez指出，攻擊者主要利用 GitHub 的評論和通知功能，並透過 `notifications@github[.]com` 發送釣魚郵件，在這次事件中，使用2個假冒的網域名稱：

- Githubcareers[.]online
- Githubcareers[.]online

在此次事件前，今年也有多起相關 Github 資安事件：

- 2月22日 Github 使用者 CodeLife234 回報一個朋友的帳號遭駭的資安事件，該事件是由於受害者點擊一個來自釣魚郵件的連結，該郵件偽造為招聘 GitHub 開發人員職位
- Github 使用者 Mindgames 也聲稱收到來自 Github 偽造為招聘 GitHub 開發人員的釣魚信，寄件者被偽造為 `notification@github[.]com`
- 另一位 Github 使用者回報稱收到一個偽造為 Github 通知系統發送的釣魚郵件，內容是告知受害者其帳號資料已經外洩，並提供連結以引導受害者至釣魚網站：
[https://githubcareer\[.\]online](https://githubcareer[.]online)
- Fernández 指出在 4 月 11 日的一個敲詐勒索的螢幕截圖，內容為 Gitloker 威脅一家 B2C 的公司，並聲稱已經竊取其資料，如不給 25 萬美金則會公開公司內部機密資料

而Github並不是第一次被針對作為攻擊的目標：

- 2020年3月，發現駭客自 2018 年 6 月以來持續攻擊微軟的帳號，並從其員工 Redmond 的私人專案儲存庫獲取超過 500

GB 的檔案

- 2020 年 9 月，Github 警告存在針對使用者的釣魚攻擊，該次攻擊透過偽造 CircleCI 發送釣魚郵件給使用者，來竊取受害者的 Github 憑證

Github 建議受害的使用者採取以下措施：

- 更換密碼
- 檢查活動紀錄
- 檢查自己的訪問權杖 (Access Token)
- 檢查授權的 OAuth 應用程式
- 不要點擊授權任何不明來源的 OAuth 應用程式授權請求

為了防止帳號被入侵，可參考下列建議：

- 啟用雙因子身分驗證
 - 檢查過去授權的 ssh key
 - 定期查看每個專案儲存庫最近的提交內容
- 資料來源：
 1. [GitHub Repos Targeted in Cyber-Extortion Attacks](#)
 2. [New Gitloker attacks wipe GitHub repos in extortion scheme](#)

2.3.2 Phoenix UEFI 漏洞影響多款 Intel CPU 設備



Phoenix SecureCore UEFI 韌體上發現了一個新漏洞 (CVE-2024-0762) ，該漏洞可能會影響可信賴平台模組 (Trusted Platform Module, TPM) 配置，從而導致緩衝區溢位和潛在惡意程式碼的執行。許多搭載 Intel CPU 的設備都會受到影響，Phoenix Technologies 強烈建議將這些韌體更新到最新版本。

資安廠商 Eclipsium 首先在 Lenovo ThinkPad 筆記型電腦上發現該漏洞，後來 Phoenix Technologies 確認此漏洞也會影響多個在 Intel 處理器上運行 SecureCore 韌體的設備，包括 AlderLake、CoffeeLake、CometLake、IceLake、JasperLake、KabyLake、MeteorLake、CometLake、IceLake、JasperLake、KabyLake、MeteorLake、MeteorLake、RaptorLake、RocketLake 和 TigerLake。換句話說，Lenovo、Dell、Acer、HP 的大量機型都受到此漏洞的影響。

CVE-2024-0762 漏洞源自於 Phoenix SecureCore 韌體的系統管理模式 (System Management Mode, SMM) 子系統內的緩衝區溢位，由於安全開機 (Secure Boot) 讓攻擊者更難安裝長駐性的惡意軟體和驅動程式，這導致更多 Bootkit 的惡意軟體針對 UEFI 的漏洞進行攻擊。

Bootkit在整個UEFI啟動的過程中很早的階段就被載入，這不僅讓惡意程式可以在底層進行操作，也大幅增加它的隱蔽性，例如UEFI的惡意軟體BlackLotus、CosmicStrand。需要注意的是，這次的漏洞發生在處理TPM組態的UEFI 程式碼中，因此 TPM 晶片將失去保護的作用。儘管 UEFI 韌體具有安全開機功能，但 Bootkit 在啟動過程中很早就加載，這可能導致電腦允許攻擊者覆蓋相鄰記憶體並獲得特權和程式碼執行的權限。

Phoenix 已於 2024 年 5 月針對漏洞提供韌體更新版本，但可能並非包含所有的型號。建議使用者應升級到最新的韌體版本，注意是否有更新資訊，或聯繫供應商以提供相關協助。

● 資料來源：

1. <https://www.bleepingcomputer.com/news/security/phoenix-uefi-vulnerability-impacts-hundreds-of-intel-pc-models/>
2. <https://www.phoenix.com/security-notifications/cve-2024-0762/>
3. <https://www.helpnetsecurity.com/2024/06/21/cve-2024-0762/>

2.4 軟硬體漏洞資訊

2.4.1 Check Point VPN Gateway存在高風險安全漏洞

CVE 編號	CVE-2024-24919
影響產品	Check Point VPN Gateway
解決辦法	官方已針對漏洞釋出修補程式，請參考官方說明進行修補，網址如下： https://support.checkpoint.com/results/sk/sk182336

- 內容說明：

研究人員發現 Check Point VPN Gateway 存在路徑遍歷(Path Traversal) 漏洞(CVE-2024-24919)，未經身分鑑別之遠端攻擊者可發送偽造請求取得任意系統檔案。該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台：

影響產品：
CloudGuard Network、Quantum Maestro、Quantum Scalable Chassis、Quantum Security Gateways 及 Quantum Spark Appliances

影響版本：
R77.20(EOL)、R77.30(EOL)、R80.10(EOL)、R80.20(EOL)、R80.20.x、R80.20SP(EOL)、R80.30(EOL)、R80.30SP(EOL)、R80.40(EOL)、R81、R81.10、R81.10.x 及 R81.2
- 資料來源：
 1. <https://nvd.nist.gov/vuln/detail/CVE-2024-24919>
 2. <https://support.checkpoint.com/results/sk/sk182336>
 3. <https://www.truesec.com/hub/blog/check-point-ssl-vpn-cve-2024-24919-from-an-incident-response-perspective>
 4. <https://www.greynoise.io/blog/whats-going-on-with-checkpoint-cve-2024-24919>

2.5.2 PHP存在高風險安全漏洞

CVE 編號	CVE-2024-4577
影響 產品	PHP
解決 辦法	<p>1.官方已針對漏洞釋出修復更新，請更新至以下版本：</p> <p>PHP 8.3 分支請更新至 8.3.8(含)以上版本</p> <p>PHP 8.2 分支請更新至 8.2.20(含)以上版本</p> <p>PHP 8.1 分支請更新至 8.1.29(含)以上版本</p> <p>針對 PHP 8.0、7 及 5 官方已不再維護，建議更換至仍在維護之版本</p> <p>2.若無法更新 PHP，可參考以下緩解方式：</p> <p>https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/#1-%E5%B0%8D%E7%84%A1%E6%B3%95%E6%9B%B4%E6%96%B0-php-%E7%9A%84%E4%BD%BF%E7%94%A8%E8%80%85</p> <p>3.如使用 XAMPP for Windows 版本，可參考以下說明：</p> <p>https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/#2-%E5%B0%8D-xampp-for-windows-%E4%BD%BF%E7%94%A8%E8%80%85</p>

- 內容說明：

研究人員發現 PHP 存在引數注入(Argument Injection)漏洞(CVE-2024-4577)，未經身分鑑別之遠端攻擊者可透過特定字元序列繞過舊有 CVE-2012-1823 弱點修補後之保護，並透過引數注入等攻擊於遠端 PHP 伺服器上執行任意程式碼，請儘速確認並進行修補。
- 影響平台：

安裝於 Windows 之以下 PHP 版本：

PHP 8.3 分支：8.3.8(不含)以下版本

PHP 8.2 分支：8.2.20(不含)以下版本

PHP 8.1 分支：8.1.29(不含)以下版本

PHP 8.0 分支所有版本

PHP 7 所有版本

PHP 5 所有版本

- 資料來源：

1. [資安通報：PHP 遠端程式碼執行 \(CVE-2024-4577\) - PHP CGI 參數注入弱點](#)

2.5.3 以Chromium為基礎之瀏覽器存在安全漏洞

CVE 編號	CVE-2024-5274
影響產品	以 Chromium 為基礎之瀏覽器
解決辦法	1.請更新 Google Chrome 瀏覽器至 125.0.6422.112(含)以上版本 https://support.google.com/chrome/answer/95414?hl=zh-Hant 2.請更新 Microsoft Edge 瀏覽器至 125.0.2535.67(含)以上版本 https://support.microsoft.com/zh-tw/topic/microsoft-edge-%E6%9B%B4%E6%96%B0%E8%A8%AD%E5%AE%9A-af8aaca2-1b69-4870-94fe-18822dbb7ef1 3.請更新 Vivaldi 瀏覽器至 6.7.3329.35(含)以上版本 https://help.vivaldi.com/desktop/install-update/update-vivaldi/ 4.請更新 Brave 瀏覽器至 1.66.115(含)以上版本 https://community.brave.com/t/how-to-update-brave/384780 5.請更新 Opera stable 瀏覽器至 110.0.5130.39(含)以上版本 https://help.opera.com/en/latest/crashes-and-issues/

- 內容說明：
 研究人員發現 Google Chrome、Microsoft Edge、Vivaldi、Brave 及 Opera 等以 Chromium 為基礎之瀏覽器存在類型混淆(Type Confusion) 漏洞(CVE-2024-5274)，遠端攻擊者可藉由利用此漏洞於沙箱內執行任意程式碼，該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台：
 Google Chrome 125.0.6422.112(不含)以下版本
 Microsoft Edge(Based on Chromium) 125.0.2535.67(不含)以下版本
 Vivaldi 6.7.3329.35(不含)以下版本

Brave 1.66.115(不含)以下版本

Opera stable 110.0.5130.39(不含)以下版本

● 資料來源：


1. <https://nvd.nist.gov/vuln/detail/CVE-2024-5274>
2. <https://support.microsoft.com/zh-tw/topic/microsoft-edge-%E6%9B%B4%E6%96%B0%E8%A8%AD%E5%AE%9A-af8aac>
3. <https://support.google.com/chrome/answer/95414?hl=zh-Hant>
4. <https://help.vivaldi.com/desktop/install-update/update-vivaldi/>
5. <https://community.brave.com/t/how-to-update-brave/384780>
6. <https://community.brave.com/t/how-to-update-brave/384780>
7. https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html
8. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5274>
9. <https://vivaldi.com/blog/desktop/minor-update-seven-6-7/>
10. <https://community.brave.com/t/release-channel-1-66-115/550022>
11. <https://blogs.opera.com/desktop/2024/05/opera-110-0-5130-39-stable-update/>

第 3 章、資安研討會及活動

【限定資訊服務業者參與】2024-03-26 ~ 2024-09-30 個人資料檔案安全維護計畫一對一線上健檢諮詢

活動時間	2024-03-26 ~ 2024-09-30
活動地點	線上活動
活動網站	https://www.cisnet.org.tw/Course/Detail/5286
活動概要	 <p>【活動內容 / Event Details】</p> <p>數產署於 2024 年 10 月 12 日訂定「數位經濟相關產業個人資料檔案安全維護管理辦法」，業者若未採取適當安全維護措施致個資被竊取、竄改、毀損、滅失或洩漏，或未訂定安全維護計畫，可處 2 萬元以上 200 萬元以下罰鍰！</p> <p>為協助資訊服務業者遵循《數位經濟相關產業個人資料檔案安全維護管理辦法》，建立個資檔案安全維護管理計畫，數產署提供線上免費個資健檢諮詢，名額有限，敬請把握。</p> <p>【指導單位】 數位發展部數位產業署</p> <p>【主辦單位】 財團法人資訊工業策進會</p> <p>【執行單位】 中華民國資訊軟體協會</p> <p>【聯絡窗口】 02-2553-3988 分機 816 林專員</p> <p>security@cisnet.org.tw</p>

【資安學院】7/2 資安稽核實務案例

活動時間	2024-07-02 09:00 ~ 2024-07-02 16:00
活動地點	中華民國資訊軟體協會-大同辦公室D01大會議室 (台北市中山區中山北路3段22-1號新設工大樓 5樓 C區)
活動網站	https://www.cisnet.org.tw/Course/Detail/5255
活動概要	 <p>【費用】 原價：NT 6,900元/人 早鳥價：NT 6,200元/人(課前一個月報名) 軟協會員價：NT 5,600元/人 費用含稅、教材、餐點及完課證明</p> <p>【活動內容 / Event Deals】 採用互動式教學，講解資安稽核實務及技巧，以及資通、金融、個資安全等相關法規之重點。運用風險評鑑方法，帶您識別組織內資訊流，依次探討系統變更管理、雲端管理、物聯網管理、網路管理、加密管理、存取控制等IT管理區塊，改善及強化組織之資安並達成合規要求，以提升學員的資安管理及稽核能力。 本課程包含：資安稽核計畫撰寫、資安稽核整備作業、資安稽核啟始會議、資安稽核軌跡設計與抽樣檢視技巧、資通安全策略面、管理面及技術面向之資安稽核重點、資安稽核報告撰寫實務及資安稽</p>

核結束會議等內容。

【主辦單位】 中華民國資訊軟體協會

【聯絡窗口】

02-2553-3988 分機 816 林專員 security@cisanet.org.tw

【報名截止】 2024-06-25

【資安學院】7/13、7/20 iPAS-「中級」資訊安全工程師-能力研習衝刺班
活動時間 2024-07-13 09:00~16:00 、 2024-07-20 09:00~16:00

活動地點 中華民國資訊軟體協會-大同辦公室D01大會議室 (台北市中山區中山北路3段22-1號新設工大樓 5樓 C區)

活動網站 <https://www.cisnet.org.tw/Course/Detail/5219>
活動概要

【費用】

原價：NT 10,500元/人

早鳥價：NT 9,500元/人(課程前一個月報名)

軟協會員：NT 8,400元/人

費用含稅、教材、餐點及完課證明

【活動內容 / Event Details】

本課程融入業界實務案例，教導您專業的資訊安全知識與技能，包含：建立符合法規與組織安全需求之系統、網路與安全防護架構、執行相關維運作業、協助其他單位執行資訊安全活動。課程中亦透過歷屆試題講解重點觀念，協助您掌握iPAS考題趨勢及技術解析，不僅提升解題戰力，應考也更佳輕鬆！

【主辦單位】 中華民國資訊軟體協會

【聯絡窗口】 02-2553-3988 分機 816 林專員 security@cisnet.org.tw

【報名截止】 2024-07-08

【資安學院】7/23 網路封包與事件解析


活動時間	2024-07-23 09:30 ~ 2024-07-23 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.cisnet.org.tw/Course/Detail/5306

活動概要

【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、餐點及完課證明

【活動內容 / Event Details】
 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。
 本課程著重於介紹網路通訊中常用通訊協定原理、分析與應用，透過課程教學與上機實務操作，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，有效進行網路事件的資訊蒐集與封包判讀。

【主辦單位】 中華民國資訊軟體協會
【聯絡窗口】 02-2553-3988 分機 816 林專員 security@cisnet.org.tw



【報名截止】 2024-07-16

【資安學院】7/25 程式碼掃描修補技巧

活動時間	2024-07-25 09:00 ~ 2024-07-25 16:00
活動地點	中華民國資訊軟體協會-大同辦公室D01大會議室 (台北市中山區中山北路3段22-1號新設工大樓 5樓 C區)
活動網站	https://www.cisnet.org.tw/Course/Detail/5267

活動概要

>>>>

中華軟協資安學院

程式碼掃描修補技巧

系統上線前執行源碼掃描安全檢測已是常見檢測作業，檢測工具所顯示之弱點與實際程式的架構不同，真的代表有這個漏洞存在嗎？

本課程透過**實務案例**分析常見漏洞教學，原始碼掃描修補邏輯判斷的原則，並透過實務教學OWASP TOP 10 掃描風險修補技巧。

課程資訊

7/25(四)
9:00 - 16:00 (6hr)
中華民國資訊軟體協會
大同辦公室D01大會議室

適合對象

- 資安監控管理人員
- 網路管理人員
- 系統管理人員
- 資安(訊)主管

課程內容

- SSDLC 開發重點
- 原始碼掃描修補邏輯判斷的原則
- OWASP TOP 10 掃描風險修補技巧

課程費用

- 原價：NT 8,000元/人
- 早鳥價：NT 7,200元/人
- 軟協會員：**NT 6,800元/人**
- 費用含稅、教材、餐點及完課證明

講師簡介

- 現職：科技公司資安顧問
- 經歷：
 - 資訊安全工程師、講師及資安顧問等
 - 行政院國家資通安全會報-技術服務中心資安工程師
 - 中央、地方機關、學校等，資訊安全管理、網路安全及專案經驗工程師與講師

注意事項

- 每班至少10名學員始得開班授課，未達人數將退還繳交學費。
- 以上課程、內容資訊，主辦單位保留最終變更及調整之權利。

CISA 數位轉型大學
Digital Transformation University of CISA

聯絡資訊：中華軟協資安服務處 林專員
Email : security@cisnet.org.tw
Tel: (02)2553-3988 Ext : 816

>>>>

【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、餐點及完課證明

【活動內容 / Event Details】

系統上線前執行源碼掃描安全檢測已是常見檢測作業，檢測工具所顯示之弱點與實際程式的架構不同，真的代表有這個漏洞存在嗎？本課程透過實務案例分析常見漏洞教學，原始碼掃描修補邏輯判斷的原則，並透過實務教學 OWASP TOP 10 掃描風險修補技巧。

【主辦單位】 中華民國資訊軟體協會

【聯絡窗口】 02-2553-3988 分機 816 林專員 security@cisanet.org.tw

【報名截止】 2024-07-18

【資策會】7/26(五)舉辦「企業數位轉型強化資安韌性」媒合交流會，敬邀產業先進踴躍參加！

活動時間 113年07月26日(五)下午13:00~16:20 (敬備茶點)

活動地點 數位產業署沙崙資安服務基地5樓D508共創空間(地址:臺南市歸仁區歸仁13路1段6號)

活動網站 <https://ievents.iii.org.tw/EventS.aspx?t=0&id=2472>

活動概要

資安深耕及沙崙實驗計畫-智慧沙崙物聯網資安實證計畫

企業數位轉型 強化資安韌性 媒合交流會

113/7/26(五)
13:00~16:20

地點：沙崙資安服務基地5樓D508共創空間
(地址：臺南市歸仁區歸仁十三路一段6號)

物聯網資安

零信任防護

監控與應變

資安合規

近年來企業紛紛推動數位轉型來達成ESG永續經營的目標，在數位轉型階段，企業運用各種數位工具來優化企業內部設備與資料達到資訊化、雲端化及數位化，但也增加資安的風險。在每個資安事件發生都會影響環境、社會及公司治理，「資訊安全」漸漸成為企業永續治理重要的一環，企業領導者除了關注營運韌性、供應鏈韌性外，網路安全的資安韌性也是轉型中不可或缺的關鍵，本活動邀請資安專家參與，針對「物聯網資安、零信任防護、監控與應變及資安合規」等四大面向提供資安部署案例分享。

時間	議程	講者
13:00~13:35	報到/開場	沙崙計畫服務團隊
13:35~13:50	「物聯網」資安部署案例分享	中華資安國際 林峰正 經理
13:50~14:05	「零信任防護」資安部署案例分享	偉康科技股份有限公司
14:05~14:20	「監控與應變」資安部署案例分享	騰曜網路科技 彭中如 技術經理
14:20~14:35	「資安合規」部署案例分享	安基資訊 黃瓊瑩 副總經理
14:35~15:35	資安解方分組交流	全體貴賓
15:35~15:50	茶敘休息與移動到沙崙基地	全體貴賓
15:50~16:20	沙崙基地Testbed導覽	全體貴賓
16:20~	賦歸	

數位發展部數位產業署廣告

【費用】

免費

【活動內容 / Event Details】

近年來企業紛紛推動數位轉型來達成 ESG 永續經營的目標，在數位轉型階段，企業運用各種數位工具來優化企業內部設備與資料達到資訊化、雲端化及數位化，但也增加資安的風險。在每個資安事件發生都會影響環境、社會及公司治理，「資訊安全」漸漸成為企業永續治理重要的一環，企業領導者除了關注營運韌性、供應鏈韌性外，網路安全的資安韌性也是轉型中不可或缺的關鍵，本活動邀請資安專家參與，針對「物聯網資安、零信任防護、監控與應變及資安合規」等四大面向提供資安部署案例分享。

【活動對象】

推動數位轉型中，正在尋找「資安解決方案」的領域廠商

【活動目標】

協助智慧製造的業者在面臨眾多資安議題與解決方案時，如何依自身需求評選、規劃及導入合適的資安解決方案

【主辦單位】 數位發展部數位產業署

【聯絡窗口】 (06)303-2260#535 張小姐 changyunyun@iii.org.tw

【報名截止】 2024-07-22

【資安學院-國際證照班】8/15-8/16、8/21-8/23 ISO 27001：2022資訊安全管理系統主導稽核員訓練課程

活動時間	2024-08-15 09:00 ~ 2024-08-23 18:30
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.cisanel.org.tw/Course/Detail/5177
活動概要	 <p>【費用】 原價：NT 56,000元/人 軟協會員/公家機關：請洽承辦人員 費用含稅、教材、餐點及證書</p> <p>【活動內容 / Event Details】 課程內容結合了個別單元之介紹、個案研究、實務案例研討、聯合測驗及角色扮演的融合群組討論。課程設計是為了訓練參加者有能力成為符合國際稽核準則之 ISO/IEC 2001:2022 合格稽核員。參加者將行課程中得到如何協助組織建立、稽核 ISO/IEC 27001:2022 資訊安全管理系統並通過驅證取得國際課程證照。</p> <p>【主辦單位】 中華民國資訊軟體協會 【聯絡窗口】 02-2553-3988 分機 816 林專員 security@cisanel.org.tw 【報名截止】 2024-08-08</p>

【資安學院-國際證照班】9/2 BS 10012:2017+A1:2018 個人資訊管理系統
基礎課程
活動時間 2024-09-02 09:00 ~ 2024-09-02 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.cisnet.org.tw/Course/Detail/5177>
活動概要
【費用】

原價：NT 8,500元/人

軟協會員/公家機關：請洽承辦人員

早鳥價：NT 8,450元/人(開課前兩個月需完成報名及繳費)

費用含稅、教材、餐點及證書

【活動內容 / Event Deails】

本課程為學習個人資訊管理系統 (PIMS) 的最佳入門課程。學員可經由課程了解個人資訊的重要性，讓各個規模的組織在短時間內瞭解個資管理系統，及國內法令法規要求，對資料保護原則及範圍有初步且正確的認知。並且能協助組織達到加深完善個資管理作業流程及正確因應新版個資法之益處。

【主辦單位】 中華民國資訊軟體協會

【聯絡窗口】 02-2553-3988 分機 816 林專員 security@cisnet.org.tw

【報名截止】 2024-08-26


第 4 章、TVN 漏洞公告

TWCERT/CC 本月份發布之CVSS 3分數為8.8以上之漏洞資訊如下表：

鼎新電腦 EasyFlow .NET - SQL Injection	
TVN / CVE ID	TVN-202406001 / CVE-2024-5311
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	EasyFlow .NET V5.x, V6.1.x, V6.6.x
問題描述	鼎新電腦 EasyFlow .NET 之部分功能參數未對使用者輸入進行驗證，未經身分鑑別之遠端攻擊者可注入任意 SQL 指令以讀取、修改及刪除資料庫內容。
解決方法	V5.x 與 V6.1.x 請安裝修補程式(2024/02/01或之後釋出的版本) V6.6.x 請更新至 V6.6.16(含)以後版本
公開日期	2024-06-03
相關連結	https://www.twcert.org.tw/tw/cp-132-7844-52dad-1.html

ASUS 路由器 - Improper Authentication	
TVN / CVE ID	TVN-202406003 / CVE-2024-3080
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	ZenWiFi XT8 3.0.0.4.388_24609(含)以前版本 ZenWiFi XT8 V2 3.0.0.4.388_24609(含)以前版本 RT-AX88U 3.0.0.4.388_24198(含)以前版本 RT-AX58U 3.0.0.4.388_23925(含)以前版本

	RT-AX57 3.0.0.4.386_52294(含)以前版本 RT-AC86U 3.0.0.4.386_51915(含)以前版本 RT-AC68U 3.0.0.4.386_51668(含)以前版本
問題描述	ASUS部分路由器型號存在鑑別繞過漏洞，允許未經身分鑑別之遠端攻擊者登入設備。
解決方法	更新 ZenWiFi XT8 至 3.0.0.4.388_24621(含)以後版本 更新 ZenWiFi XT8 V2 至 3.0.0.4.388_24621(含)以後版本 更新 RT-AX88U 至 3.0.0.4.388_24209(含)以後版本 更新 RT-AX58U 至 3.0.0.4.388_24762(含)以後版本 更新 RT-AX57 至 3.0.0.4.386_52303(含)以後版本 更新 RT-AC86U 至 3.0.0.4.386_51925(含)以後版本 更新 RT-AC68U 至 3.0.0.4.386_51685(含)以後版本
公開日期	2024-06-14
相關連結	https://www.twcert.org.tw/tw/cp-132-7859-0e104-1.html

飛騰雲端 HR Portal - Insufficient Session Expiration

TVN / CVE ID	TVN-202406009 / CVE-2024-5995
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
影響產品	HR Portal 7.3.2024.0409(不含)以前版本
問題描述	飛騰雲端 HR Portal 寄出之通知信件含有附帶 session 的連結，該 session 的時效性並未被妥善設定，有效性可長達7日以上且可重複利用。
解決方法	更新至 7.3.2024.0409(含)以後版本
公開日期	2024-06-14

相關連結	https://www.twcert.org.tw/tw/cp-132-7871-fecf1-1.html
------	---

飛騰雲端 HR Portal - Cleartext Transmission of Sensitive Information	
TVN / CVE ID	TVN-202406010 / CVE-2024-5996
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
影響產品	HR Portal 7.3.2024.0409(不含)以前版本
問題描述	飛騰雲端 HR Portal 寄出之通知信件含有附帶 session 的連結，其寄信時並未使用加密的傳輸協定，若攻擊者從中攔截封包可取得該 session 明文資訊，並利用此 session 登入系統。
解決方法	更新至 7.3.2024.0409(含)以後版本
公開日期	2024-06-14
相關連結	https://www.twcert.org.tw/tw/cp-132-7873-5ba4c-1.html

ASUS 路由器 - Upload arbitrary firmware	
TVN / CVE ID	TVN-202406011 / CVE-2024-3912
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	DSL-N17U, DSL-N55U_C1, DSL-N55U_D1, DSL-N66U, DSL-N14U, DSL-N14U_B1, DSL-N12U_C1, DSL-N12U_D1, DSL-N16, DSL-AC51, DSL-AC750, DSL-AC52U, DSL-AC55U, DSL-AC56U
問題描述	ASUS 路由器部分型號存在任意韌體上傳漏洞，未經身分鑑別之遠端攻擊者可利用此漏洞於設備上執行任意系統指令。
解決方法	將以下型號更新至 1.1.2.3_792(含)以後

	<p>版本： DSL-N17U, DSL-N55U_C1, DSL-N55U_D1, DSL-N66U</p> <p>將以下型號更新至1.1.2.3_807(含)以後</p> <p>版本： DSL-N12U_C1, DSL-N12U_D1, DSL-N14U, DSL-N14U_B1</p> <p>將以下型號更新至1.1.2.3_999(含)以後</p> <p>版本： DSL-N16, DSL-AC51, DSL-AC750, DSL-AC52U, DSL-AC55U, DSL-AC56U</p> <p>以下型號已不再維護，建議進行汰換 DSL-N10_C1, DSL-N10_D1, DSL-N10P_C1, DSL-N12E_C1, ,DSL-N16P, DSL-N16U, DSL-AC52, DSL-AC55</p> <p>若短期內無法汰換，建議關閉遠端存取 (Web access from WAN), 虛擬伺服器 (Port forwarding), DDNS, VPN 伺服器, DMZ, 通訊埠觸發程式(port trigger)</p>
公開日期	2024-06-14
相關連結	https://www.twcert.org.tw/tw/cp-132-7875-872d3-1.html

GeoVision 已停止維護之設備 - OS Command Injection

TVN / CVE ID	TVN-202406015 / CVE-2024-6047
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	DSP LPR : GV_DSP_LPR_V2

	IP Camera : GV_IPCAMD_GV_BX1500 GV_IPCAMD_GV_CB220 GV_IPCAMD_GV_EBL1100 GV_IPCAMD_GV_EFD1100 GV_IPCAMD_GV_FD2410 GV_IPCAMD_GV_FD3400 GV_IPCAMD_GV_FE3401 GV_IPCAMD_GV_FE420 Video Server : GV-VS14_VS14 GV_VS03 GV_VS2410 GV_VS28XX GV_VS216XX GV VS04A GV VS04H DVR : GVLX 4 V2 GVLX 4 V3
問題描述	GeoVision部分已停止支援設備之特定功能未妥善過濾使用者輸入，未經身分鑑別之遠端攻擊者可利用此漏洞注入系統指令並於設備上執行。
解決方法	產品已不再維護，建議汰換設備
公開日期	2024-06-17
相關連結	https://www.twcert.org.tw/tw/cp-132-7875-872d3-1.html

網擎資訊 MailGates 與 MailAudit - OS Command Injection

TVN / CVE ID	TVN-202406016 / CVE-2024-6048
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

影響產品	MailGates 5.0/6.0、MailAudit 5.0/6.0
問題描述	網擎資訊MailGates與MailAudit在分析信件附件時未妥善過濾使用者輸入，未經身分鑑別之遠端攻擊者可利用此漏洞注入系統指令並於遠端伺服器上執行。
解決方法	更新 MailGates/MailAudit v5.0 至 Patch 5.2.10.094(含)以後版本 更新 MailAudit/MailAudit v6.0 至 Patch 6.1.7.037(含)以後版本
公開日期	2024-06-17
相關連結	https://www.twcert.org.tw/tw/cp-132-7885-a8013-1.html

編輯：TWCERT/CC 團隊

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：2024年 6月 28 日

電子郵件：CERT_Service@cert.org.tw

官網：<https://twcert.org.tw/>

Facebook 粉絲專頁：<https://www.facebook.com/twcertcc/>

Instagram：<https://www.instagram.com/twcertcc/>