TWCERT/CC 資安情資電子報

2024 年 9 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。範疇可能包含資訊安全宣導、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

駭客組織攻擊台灣網站，政府、財稅單位為首要目標 1

第 2 章、國內外重要資安事件 5

2.1 新興應用資安 5

2.1.1 ArtiPACKED:潛在的 GitHub Actions 安全風險 5

2.2 資安趨勢 8

2.2.1 Github 評論功能成為傳播惡意程式管道 8

2.3 軟硬體漏洞資訊 11

2.3.1 Dahua IP Camera存在高風險安全漏洞 11

2.3.2 兆勤科技部分無線基地台和資安路由器設備存在重大安全漏洞 13

2.3.3 SonicOS存在高風險安全漏洞 14

第 3 章、資安研討會及活動 15

第 4 章、TVN 漏洞公告 24

編輯：TWCERT/CC 團隊 30

第 1 章、封面故事

駭客組織攻擊台灣網站，政府、財稅單位為首要目標

近期，駭客組織NoName057和RipperSec因政治因素，聲稱其已對台灣多個網站發起分散式阻斷服務(Distributed Denial-of-Service, DDoS)攻擊。第一波攻擊目標以政府機關為主，隨後財稅單位、金融機關及部分企業也陸續受到影響。

分散式阻斷服務攻擊是一種常見的網路攻擊手法，攻擊者利用受控的殭屍網路裝置，對目標伺服器發起大規模流量或資源消耗攻擊，使伺服器因無法負荷而無法正常提供服務。此次，NoName057宣稱使用名為「DDoSia」的工具，透過HTTPs Flood及TCP SYN Flood等方式攻擊台灣網站。這類型的攻擊，是利用三向交握的網路連線機制，傳送偽冒來源IP的SYN封包，使伺服器回應偽造IP位址，

於伺服器等待回應的期間，攻擊者仍會大量持續傳送SYN請求封包，而偽冒來源IP的封包使得伺服器無法順利收到回覆，並佔用大量伺服器連接埠，導致正常用戶無法連線。

針對此類DDoS攻擊，企業可以採取以下幾種防護措施來降低攻擊對服務的影響：

- 防火牆 (Firewall)：作為基本防護，防火牆能有效阻擋特定協定、Port及IP等異常流量。隨著大數據及人工智慧技術的應用，近期的防火牆較能識別異常流量，並在不影響正常流量的前提下，阻擋DDoS攻擊，或在防火牆上開啟地理IP(Geo-IP)過濾功能，設定阻擋特定國家或地區的IP地址範圍，避免不必要的跨境連線，可以有效降低潛在攻擊來源的影響。
- 應用程式防火牆(WAF)：WAF能監控進入網站的HTTP和HTTPS請求，通過設置特定的閾值來監測每個來源的請求頻率。當來自單一IP或多個IP的請求在短時間內異常增加並超出正常範圍時，可識別為HTTPs Flood攻擊，並採取相應措施。
- 入侵防禦系統 (Intrusion-Prevention Systems, IPS)：透過比對特徵碼，IPS能阻擋異常流量，針對SYN Flood及應用層DDoS攻擊進行特定防護。
- 交換器 (Switch)：具備速率限制與存取控制(Access Control List, ACL)功能，並能透過Traffic Shaping機制防禦低速緩慢攻擊及SYN Flood等DDoS攻擊。
- 路由器 (Router)：利用速率限制及存取控制等功能，啟用入口過濾(Ingress Filtering)機制，檢測並過濾偽造IP位址的攻擊流量，如SYN Flood攻擊。
- 網路流量清洗 (Flow Cleaning)：由服務提供商建立的流量清洗機制，能針對常見的DDoS攻擊類型，如SYN Flood、應用層DDoS

攻擊及低速攻擊，提供乾淨的網路環境，保障服務不中斷。

資安業者Sekoia指出，DDoSia工具是NoName057等駭客組織發動DDoS攻擊的核心工具之一，駭客透過C2(Command and Control)伺服器發送指令給殭屍電腦，以大量的惡意流量來癱瘓目標伺服器，這些C2伺服器及殭屍電腦分佈在全球，駭客利用受控設備來進行多點攻擊。為了減少這類攻擊的影響，Sekoia整理了相關的C2伺服器IP清單，企業可將此IP加入相關資安設備，以進行偵測或阻擋來自外部的惡意流量，也能防止內部的電腦因感染惡意軟體而遭駭客操控，進而成為殭屍網路的一部分，參與對外發動攻擊。

IPv4	Date of activation (YYYY/MM/DD)	Host country	Autonomus System (AS)	ASN
38.180.95[.]29	2024-02-23	Hong Kong	M247	AS9009
38.180.101[.]98	2024-02-22	Serbia	M247	AS9009
185.39.204[.]86	2024-02-22	Turkey	GIR-AS	AS207713
195.133.88[.]73	2024-02-21	Germany	GIR-AS	AS207713
185.239.48[.]70	2024-02-21	Israel	IL	AS42474
5.252.23[.]100	2024-02-20	Slovakia	STARK-INDUSTRIES	AS44477
193.17.183[.]18	2024-02-19	Spain	NEARIP	AS49600
193.233.193[.]65	2024-02-12	Hong Kong	ADCDATACOM-AS-AP	AS135330
77.75.230[.]221	2024-02-10	Czech Republic	STARK-INDUSTRIES	AS44477
185.234.66[.]239	2024-02-09	Turkey	STARK-INDUSTRIES	AS44477
83.217.9[.]33	2024-02-08	Turkey	GIR-AS	AS207713
83.217.9[.]48	2024-02-08	Turkey	GIR-AS	AS207713
193.187.175[.]252	2024-02-08	France	CLOUDBACKBONE	AS56971
45.84.0[.]235	2024-02-08	Moldova	STARK-INDUSTRIES	AS44477
45.136.199[.]235	2024-02-07	Romania	M247	AS9009
185.234.66[.]126	2024-02-06	Turkey	STARK-INDUSTRIES	AS44477
193.233.193[.]90	2024-02-04	Hong Kong	ADCDATACOM-AS-AP	AS135330

45.89.55[.]4	2024-02-02	Serbia	STARK-INDUSTRIES	AS44477
188.116.20[.]254	2024-02-01	Kazakhstan	ASNLS	AS200590
77.83.246[.]159	2024-01-31	Poland	GIR-AS	AS207713
185.255.123[.]84	2024-01-29	Nigeria	BrainStorm Network	AS136258
195.35.19[.]138	2024-01-26	Brazil	AS-HOSTINGER	AS47583
89.105.201[.]91	2024-01-23	Netherlands	NOVOSERVE-AS	AS24875
5.44.42[.]29	2024-01-23	United Arab Emirates	GIR-AS	AS207713
193.233.193[.]240	2024-01-22	Hong Kong	ADCDATACOM-AS-AP	AS135330
94.131.97[.]202	2024-01-20	Czech Republic	STARK-INDUSTRIES	AS44477
94.140.115[.]89	2023-10-26	Latvia	NANO-AS	AS43513
94.140.115[.]92	2023-07-05	Latvia	NANO-AS	AS43513
77.75.230[.]221	2023-05-15	Czech Republic	STARK-INDUSTRIES	AS44477
161.35.199[.]2	2023-02-10	Germany	DIGITALOCEAN-ASN	AS14061
212.73.134[.]208	2023-01-27	Bulgaria	NETERRA-AS	AS34224
94.140.114[.]239	2023-01-10	Latvia	NANO-AS	AS43513

- 資料來源：
  1. Pro-Russian hackers launch DDoS attack over Lai comments: cybersecurity firm
  2. NoName057(16)’s DDoSia project: 2024 updates and behavioural shifts
  3. 分散式阻斷服務攻擊(DDoS)趨勢與防護

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 ArtiPACKED:潛在的 GitHub Actions 安全風險

近期Palo Alto Networks Unit 42資安研究員Yaron Avital在 GitHub Actions artifacts 發現的一種名為「ArtiPACKED」的攻擊手法 ，此攻擊可能由於Github Actions 使用不安全的設定、錯誤的設定，而導致第三方雲端服務與Github Token外洩，使攻擊者可以利用這些資訊接管整個儲存庫，甚至取得組織的雲端環境存取權限。

Github Action是Github提供的一項CI/CD服務，透過自動化的流程不僅降低錯誤率和提升維護品質，還可以同時縮短開發時間並提高效率。CI(持續整合，Continuous Integration)是指開發的程式碼送出後，會經過自動化的測試及驗證，以確保程式在正式環境上可以正常運作；CD(持續部署，Continuous Deployment)則是程式通過測試後，自動將其部署到正式環境中。以上的服務，不僅使應用程式快速更新且頻繁地發布，還能減少了手動部署過程中的錯誤。

Yaron Avital發現在Github Action的過程中，測試或執行檔案所產生Artifacts檔案，可用於在同一個工作流程中與其它的工作項目共享日誌記錄、測試結果或二進位檔案等資料。由於這些資料是公開的，並且會保留90天，這意味者攻擊者可能藉此讀取這些檔案，取得敏感資訊，其中包括 GITHUB_TOKEN 及 ACTIONS_RUNTIME_TOKEN，攻擊者即可進一步利用前述的Token進行攻擊活動。

在GitHub 中，經常出現兩種類型的 Token：

- GITHUB_TOKEN：是一個自動產生的憑證，用於在 GitHub Actions 工作流程中，執行針對儲存庫的認證操作。每次執行 GitHub Actions 工作流程時，GitHub 會自動產生一個 GITHUB_TOKEN，並將其設置為工作流程的環境變數。雖然 GITHUB_TOKEN 會在工作流程結束時過期，但由於 Artifacts 功能在版本 4 中的提升速度的攻擊，攻擊者可以利用競爭條件(race condition)的情況，在工作流程運行過程中下載 Artifacts，從而竊取並使用這些 Token。
- ACTIONS_RUNTIME_TOKEN：是一個JSON Web Token (JWT)，通常由 GitHub Actions 在執行工作流程時自動產生。這個 Token 通常用於內部的工作流程管理，如 Artifacts 的上傳(actions/upload-artifact)和快取(actions/cache)，其有效期長達六小時。如果在此期間，攻擊者能夠成功取得 Token，便可能利用該 Token 來執行惡意操作。

以下二種使用方式也可能導致Token被公開，使用者需要額外注意：

- 使用Github基本功能時，如checkout進行clone，使用者忽略使用該功能後，GITHUB_TOKEN 將被寫入本機以便執行git命令，

使用者不經意將含有Token的隱藏.git檔上傳至公開Github儲存庫。

- 代碼檢查器Super-linter的log file會紀錄許多細節也替工程師提供資訊且解決問題，例如log file儲存含有Token的環境參數。當CREATE_LOG_FILE屬性被設置為True時，該操作可能導致軟體暴露在危險中。目前，Super-linter已經將環境參數從log file移除。

另外，Yaron Avital 提到，許多使用者對於 Artifact 掃描的意識普遍不足，並建議應掃描檔案中是否含有敏感資訊作為防禦此類攻擊，因此也呼籲使用者在每一個環節中都應考慮潛在的威脅，因為被利用的威脅往往是那些被忽略的小細節。事實上，許多大型知名科技公司，如 Amazon Web Services（AWS）、Google、Microsoft、Red Hat 和 Ubuntu，都面臨這種隱藏的問題。GitHub 也表示，企業應自行負責管理和保護Artifacts，以有效防範潛在的安全風險。

- 資料來源：
  1. ArtiPACKED: Hacking Giants Through a Race Condition in GitHub Actions Artifacts
  2. GitHub Vulnerability 'ArtiPACKED' Exposes Repositories to Potential Takeover

2.2 資安趨勢

2.2.1 Github 評論功能成為傳播惡意程式管道

GitHub項目問題(Issue)的評論功能遭到濫用，駭客利用該功能傳播Lumma Stealer惡意程式，使用者應留意Github上的任何檔案與連結，若有不慎遭攻擊成功，應儘速更換帳號密碼，以確保個人電腦使用安全。

此次事件最早是由一位維護Rust函式庫:teloxide的人員在Reddit論壇上提出，發現其維護的函式庫中的評論出現偽裝修復程式，實際上為惡意程式的留言內容。

下圖為駭客散播惡意程式的評論範例，顯示民眾可透過bit.ly或mediafire 連結來下載修復程式，且在目前觀察到的評論中，密碼皆使用changeme。

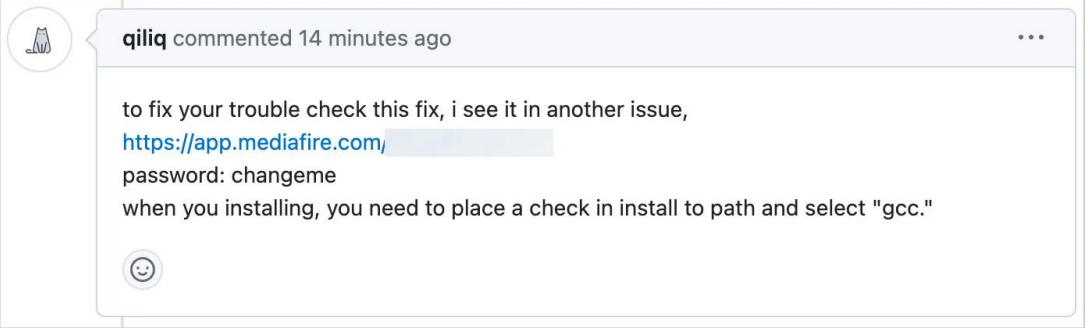


圖1 駭客散播惡意程式的評論，圖片取自 BleepingComputer

若點擊圖1的連結就會下載 fix.zip ，解壓縮後為圖2的內容，將其丟入 AnyRun 惡意程式分析沙箱平台，即能識別為Lumma Stealer 惡意程式。

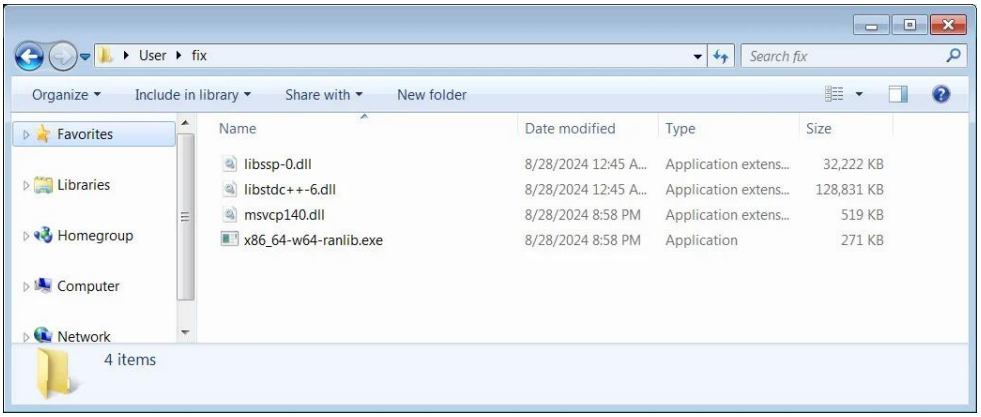


圖2 含有 Lumma Stealer 惡意程式的檔案，圖片取自 BleepingComputer

Lumma Stealer惡意程式是一種竊取資料的惡意程式，將竊取使用者的瀏覽器裡儲存的 Cookie、憑證、信用卡、密碼、瀏覽紀錄等，並將竊取的資料傳回饋予攻擊者，而後攻擊者可以利用這些資料進行下一階段的攻擊，或將其販賣於地下市場。

資安研究人員Nicholas Sherlock指出過去 3 天觀察到超過 29,000 個評論在 Github上散播Lumma Stealer惡意程式，Github管理人員亦表示已經有檢測到這些評論並將其刪除，但在Reddit仍持續有發現民眾留言表示遭受攻擊。

上個月Check Point研究人員發出一份報告，其有關駭客組織Stargazer

Goblin 利用Github上有3,000多個假帳號遭利用來散播惡意程式，雖不確定是否跟此次事件有關，但使用者須小心謹慎對待Github上的任何檔案和連結，若有使用者有遭受此攻擊，應儘速更換所有帳號的密碼，來確保個人電腦使用安全。

- 資料來源：

1. GitHub comments abused to push password stealing malware masked as fixes
2. PSA: LummaC2 Trojan Stealer spreading on GitHub issues
3. Stargazers Ghost Network - Check Point Research

2.3 軟硬體漏洞資訊

2.3.1 Dahua IP Camera存在高風險安全漏洞

CVE 編號	CVE-2021-33044 與 CVE-2021-33045
影響產品	Dahua IP Camera
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下： https://www.dahuasecurity.com/aboutUs/trustedCenter/details/582

- 內容說明：

  近期研究人員發現駭客針對過去發現之重大漏洞進行攻擊，部分 Dahua IP Camera 存在驗證繞過(Authentication Bypass)漏洞(CVE-2021-33044 與 CVE-2021-33045)，遠端攻擊者可繞過身分鑑別直接登入受影響設備，請儘速確認並進行修補。

- 影響平台：

  DHI-ASI7213Y-V3-T1
  IPC-HUM7XXX
  IPC-HX1XXX
  IPC-HX2XXX
  IPC-HX3XXX
  IPC-HX5(4)(3)XXX
  IPC-HX5XXX
  IPC-HX8XXX
  NVR1XXX
  NVR2XXX
  NVR5XXX
  NVR6XX
  PTZ Dome Camera SD1A1
  PTZ Dome Camera SD22
  PTZ Dome Camera SD49

PTZ Dome Camera SD50
PTZ Dome Camera SD52C
PTZ Dome Camera SD6AL
Thermal TPC-BF1241
Thermal TPC-BF2221
Thermal TPC-BF5XXX
Thermal TPC-PT8X21B
Thermal TPC-SD2221
Thermal TPC-SD8X21
VTH542XH
VTO65XXX
VTO75X95X
XVR4xxx
XVR5xxx
XVR7xxx

- 資料來源：

1. https://nvd.nist.gov/vuln/detail/CVE-2021-33044
2. https://nvd.nist.gov/vuln/detail/CVE-2021-33045
3. https://www.dahuasecurity.com/aboutUs/trustedCenter/details/582

2.3.2 兆勤科技部分無線基地台和資安路由器設備存在重大安全漏洞

CVE 編號	CVE-2024-7261
影響產品	Windows
解決辦法	根據以下官網所提供之資訊，將路由器設備進行更新修補。 https://www.zyxel.com/tw/zh/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024

- 內容說明：

  兆勤科技(Zyxel Network)旗下部分無線基地台和資安路由器設備存在重大資安漏洞(CVE-2024-7261，CVSS v3.1：9.8)，該漏洞起因是這些設備韌體版本中 CGI 程式的 host 參數設計不當，可能導致未經身分驗證的攻擊者遠端執行作業系統命令。

- 影響平台：
  - 無線基地台型號

    NWA50AX、NWA50AX PRO、NWA55AXE、NWA90AX、NWA90AX PRO、NWA110AX、NWA130BE、NWA210AX、NWA220AX-6E、NWA1123-AC PRO、NWA1123ACv3、WAC500、WAC500H、WAC6103D-I、WAC6502D-S、WAC6503D-S、WAC6552D-S、WAC6553D-E、WAX300H、WAX510D、WAX610D、WAX620D-6E、WAX630S、WAX640S-6E、WAX650S、WAX655E、WBE530、WBE660S
  - 資安路由器

    USG LITE 60AX
- 資料來源：
  1. https://www.zyxel.com/tw/zh/support/security-advisories/zyxel-security-advisory-for-os-command-injec

2.3.3 SonicOS存在高風險安全漏洞

CVE 編號	CVE-2024-40766
影響產品	SonicWall Firewall
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下： https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

- 內容說明：

  研究人員發現 SonicOS 存在不當存取控制(Improper Access Control)漏洞(CVE-2024-40766)，允許未經授權資源存取或於特定條件下導致防火牆失效，該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：

  SonicWall Firewall Gen 5: SonicOS 5.9.2.14-12o(含)以下版本

  SonicWall Firewall Gen 6: SonicOS 6.5.4.14-109n(含)以下版本

  SonicWall Firewall Gen 7: SonicOS 7.0.1-5035(含)以下版本

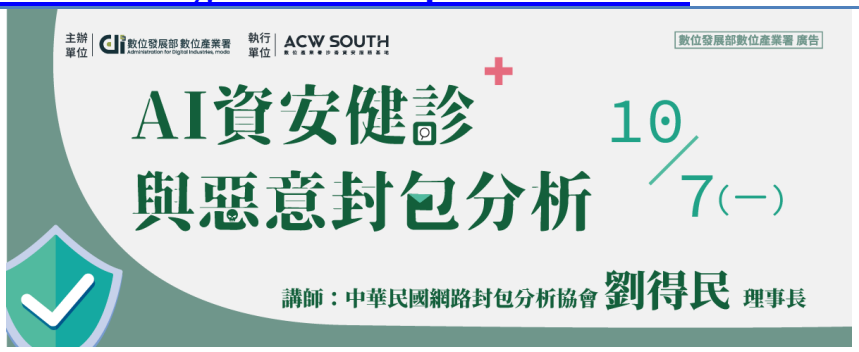
- 資料來源：

  1. https://www.zyxel.com/tw/zh/support/security-advisories/zyxel-security-advisory-for-os-command-injec
  2. https://www.cve.org/CVERecord?id=CVE-2024-40766
  3. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

第 3 章、資安研討會及活動

【資安學院】10/4惡意程式偵測、分析、防護實戰班	
活動時間	**2024-10-04 09:00 ~ 2024-10-04 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.cisanet.org.tw/Course/Detail/5257**
活動概要	 **【費用】** 原價： 6,900元/人 早鳥價： 6,200元/人(課前一個月報名) 軟協會員：5,600元/人 費用含稅、教材、餐點及完課證明 報名截止： 2024-09-27 **【活動內容 / Event Deails】** 惡意程式一向為嚴重的資安威脅，從一般的殭屍網路、勒索軟體到精密的 APT 攻擊，惡意程式都扮演重要的攻擊媒介。因此檢測系統中的惡意程式， 為相當重要的資安議題。 本課程將介紹各類型的惡意程式及結構，並從 DEMO 操作了解各種惡意程式的行為特徵，如：Backdoor、rootkit、無檔案攻擊等。了解惡意程式的行為後，課程的另一重點為探討在企業組織內部的基礎

	IT 架構中，要如何偵測惡意程式，以及主機感染惡意程式後，如何使用分析工具查找惡意程式進而清除。 **【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**
【資安院】10/5~6、10/19~20資安菁英實戰培育課程 第2期臺南場(四日)	
活動時間	**2024/10/5~6、2024/10/19~20**
活動地點	**國科會-資安暨智慧科技研發大樓 1樓會議室** **台南市歸仁區歸仁十三路一段6號(近高鐵台南站)**
活動網站	**https://nicste2.kktix.cc/events/113elitecourse2**
活動概要	 **【費用】** 免費 **【活動內容 / Event Deails】** 一直以來，全球的資訊安全事件層出不窮，從企業到國家等級的設施、甚至到作業系統都曾遭受攻擊，第二期的菁英課程除了探討ICS與逆向工程，透過更多實戰演練及工控系統實際操作，讓國際級講師帶您揭開資安攻擊與防禦的神秘面紗！ 不論您是在一般企業、政府單位、資安公司或是其他單位的在職資安技術/研發人員，都歡迎踴躍報名！此次活動將由政府全額補助，所以名額有限，千萬要把握機會喔～

	《第 2 期臺南場課程資訊》 113 年 10 月 5 日至 6 日 (週六、週日)：從零開始建構工業控制系統(ICS)的防禦工事：鄭仲倫講師 113 年 10 月 19 日(週六)：解構野外惡意程式隨開即用的瑞士刀：馬聖豪講師 113 年 10 月 20 日(週日)：網路威脅防禦競賽 **【指導單位】**數位發展部資通安全署 **【主辦單位】**國家資通安全研究院 **【執行單位】**社團法人台灣駭客協會 **【聯絡窗口】**02-2380-0923 鄭規劃師　te-atc@nics.nat.gov.tw **【報名截止】**2024-09-23 ※24 小時/4 天課程恕不接受單堂課程報名 ※報名與相關詳細資訊請點活動連結
【資策會】10/7 AI資安健診與惡意封包分析	
活動時間	**113年10月07日(一)09:30-16:30**
活動地點	**ACW SOUTH 數位產業署沙崙資安服務基地C115攻防演訓教室(臺南市歸仁區歸仁十三路一段6號)**
活動網站	**https://ievents.iii.org.tw/EventS.aspx?t=0&id=2660**
活動概要	 **【費用】** 免費 **【活動對象】** 資訊人員、網路管理人員、資安推動/應用人員 **【課程目標】**

	訓練 IT 技術人員，分析惡意程式網路活動。 **【課程重點】** ● 惡意程式與加密勒索網路活動特性 ● 企業資安事件應變處理指南 ● 雲端型態 LLM-AI、本地型態 LLM-AI 及自動解析惡意程式網路封包 ● 惡意程式與加密勒索活動實際分析練習 **【主辦單位】**數位發展部數位產業署 **【聯絡窗口】**02-6631-6633 林先生 linpinghui@iii.org.tw **【報名截止】**2024-10-04
【資安學院】10/8風險無懼．營運永續—企業IT營運持續管理實戰分析班	
活動時間	**2024-10-08 09:00 ~ 2024-10-08 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.cisanet.org.tw/Course/Detail/5280**
活動概要	 **【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：NT 5,600元/人

	費用含稅、教材、餐點及完課證明 **【活動內容 / Event Deails】** 數位環境的威脅不斷演變，當企業運用科技生產出先進的產品、提供客戶即時便利的服務、追求更高利潤的同時，亦面臨著複雜的資安挑戰，如資訊系統大當機、駭客入侵、勒索病毒等層出不窮，這些威脅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，可鑑別出威脅組織的潛在衝擊，提供具有彈性的應對計畫，以維持企業IT的持續運作。 本課程先解說營運持續相關法規與標準，接著藉由各項業界實務案例及練習題目，教導學員整合風險管理與營運衝擊分析之方法，提升分析及規劃能力。 **【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】**2024-10-01
【資安學院】10/17駭客入侵防護實務	
活動時間	**2024-10-17 09:00 ~ 2024-10-17 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.cisanet.org.tw/Course/Detail/5258**

活動概要	 **【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：NT 5,600 元/人 **【活動內容 / Event Deails】** 隨著數位時代的來臨，網路安全議題儼然已成為當代人們不得不關注的問題。網站安全的實用指南，提供全面且易於操作的解決方案。從基礎到進階層面，涵蓋各種網站所需的知識和技巧。 本課程內容先介紹基本安全措施，接著透過實務攻擊 DEMO 操作，讓您了解各種入侵思路，如：控制訪問權限、常見網站安全入侵手法等。再進一步強化系統安全，探討安全配置與即時安全監測。以深入淺出的方式，使學員在短時間內掌握駭客入侵防護的重要概念，並能藉此對網路安全有更深刻的理解，且能應用所學。 **【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】**2024-09-12

【資安院】11/2~3、11/9~10資安菁英實戰培育課程 第3期臺北場(四日)	
活動時間	**2024/11/2、3、9、10**
活動地點	**臺北創新實驗室-會議A廳**

	臺北市內湖區洲子街12號2樓(近捷運港墘站2號出口)
活動網站	**https://nicste2.kktix.cc/events/113elitecourse3**
活動概要	 **【費用】** 免費 **【活動內容 / Event Deails】** 菁英班課程舉辦到今年已經第4年了！透過國際級講師傳授資安秘技與實作，獲得一片好評，今年更增添了更多演練與實作內容，讓大家不侷限於紙上談兵，而是將所學技術與理論實際操作應用，可以把課程所學正式內化成自己的能力！ 不論您是在一般企業、政府單位、資安公司或是其他單位的在職資安技術/研發人員，都歡迎踴躍報名！此次活動將由政府全額補助，所以名額有限，千萬要把握機會喔～

《第 3 期臺北場課程資訊》	
113 年 11 月 2 日至 3 日 (週六、週日)	藍隊解壓縮 - 從零開始建構企業防禦工事：鄭仲倫講師
113 年 11 月 9 日(週六)	雲端保衛戰：藍隊的雲端安全生存指南：林殿智講師
113 年 11 月 10 日(週日)	網路威脅防禦競賽

【指導單位】數位發展部資通安全署

	【主辦單位】國家資通安全研究院 【執行單位】社團法人台灣駭客協會 【聯絡窗口】02-2380-0923 鄭規劃師　te-atc@nics.nat.gov.tw 【報名截止】2024-10-17 ※24 小時/4 天課程恕不接受單堂課程報名 ※報名與相關詳細資訊請點活動連結

TWCERT/CC 資安活動紀事	
活動名稱	**TWCERT/CC 參與亞太區 APCERT CYBER DRILL 2024 演練**
活動時間	**113.08.29**
活動概要	台灣電腦網路危機處理暨協調中心（Taiwan Computer Emergency Response Team / Coordination Center, TWCERT/CC）近期參與亞太區電腦緊急事件回應小組（Asia Pacific Computer Emergency Response Team, APCERT）於8月29日舉辦的APCERT CYBER DRILL 2024 資安演練活動，驗證了台灣在因應區域性資安威脅時的應變能力。 本次演練共有來自18個APCERT會員經濟體的22個電腦資安事件處理小組（CSIRT）參與，包括台灣、澳洲、不丹、汶萊、中國、香港、印度、日本、南韓、寮國、馬來西亞、緬甸、蒙古、菲律賓、新加坡、斯里蘭卡、泰國和越南。此外，來自伊斯蘭合作組織電腦網路危機處理小組（OIC-CERT）及非洲電腦網路危機處理小組（AfricaCERT）的3個合作夥伴機構成員也參與了此次演練。

	本次資安演練主題為「應變APT組織攻擊：威利在哪裡？（APT Group Attack Response: Where is Wally?）」，模擬真實世界的進階持續性威脅（APT）攻擊事件，這類攻擊以其高度複雜性和充足資源而聞名。TWCERT/CC作為台灣的代表團隊，於演練期間分析惡意程式及受害跡證，對受影響的組織提供技術協助。透過參與這次大型國際演練，提升TWCERT/CC國際情資分享流程及事件應變能力，進一步強化了台灣的資安聯防能量，並促進APCERT「透過國際合作建立安全、潔淨且可靠的亞太地區網路空間」之宗旨。

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：

凌羣電腦 OMFLOW - Broken Access Control	
TVN / CVE ID	TVN-202409019 / CVE-2024-8779
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	OMFLOW 1.1.6.0 至 1.2.1.2
問題描述	凌羣電腦OMFLOW未妥善限制修改系統設定功能之存取，允許已取得一般權限之遠端攻擊者更新系統設定或新增管理權限帳號以取得伺服器的控制權。
解決方法	更新至 1.2.1.3
公開日期	2024-09-13
相關連結	**https://www.twcert.org.tw/tw/cp-132-8075-a0d06-1.html**

D-Link 無線路由器 - Stack-based Buffer Overflow	
TVN / CVE ID	TVN-202409021 / CVE-2024-45694
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	DIR-X5460 A1 韌體 1.01, 1.02, 1.04, 1.10 版本 DIR-X4860 A1 韌體 1.00, 1.04 版本
問題描述	D-Link無線路由器部分型號之網頁服務存在Stack-based Buffer Overflow漏洞，允許未經身分鑑別之遠端攻擊者利用此漏洞於設備上執行任意程式碼。

解決方法	更新DIR-X5460 A1韌體至1.11B04(含)以後版本 更新DIR-X4860 A1韌體至1.04B05(含)以後版本
公開日期	2024-09-16
相關連結	https://www.twcert.org.tw/tw/cp-132-8080-7f494-1.html

D-Link 無線路由器 - Stack-based Buffer Overflow	
TVN / CVE ID	TVN-202409021 / CVE-2024-45694
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	DIR-X5460 A1 韌體 1.01, 1.02, 1.04, 1.10 版本 DIR-X4860 A1 韌體 1.00, 1.04 版本
問題描述	D-Link無線路由器部分型號之網頁服務存在Stack-based Buffer Overflow漏洞，允許未經身分鑑別之遠端攻擊者利用此漏洞於設備上執行任意程式碼。
解決方法	更新DIR-X5460 A1韌體至1.11B04(含)以後版本 更新DIR-X4860 A1韌體至1.04B05(含)以後版本
公開日期	2024-09-16
相關連結	https://www.twcert.org.tw/tw/cp-132-8080-7f494-1.html

D-Link 無線路由器 - Stack-based Buffer Overflow	
TVN / CVE ID	TVN-202409022 / CVE-2024-45695
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	DIR-X4860 A1 韌體 1.00, 1.04 版本

問題描述	D-Link無線路由器部分型號之網頁服務存在Stack-based Buffer Overflow漏洞，允許未經身分鑑別之遠端攻擊者利用此漏洞於設備上執行任意程式碼。
解決方法	更新DIR-X4860 A1韌體至1.04B05(含)以後版本
公開日期	2024-09-16
相關連結	https://www.twcert.org.tw/tw/cp-132-8082-f1687-1.html

D-Link 無線路由器 - Hidden Functionality	
TVN / CVE ID	TVN-202409023 / CVE-2024-45696
CVSS	8.8 (High) CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	DIR-X4860 A1 韌體 1.00, 1.04 版本 COVR-X1870 韌體 1.02(含)以下版本
問題描述	D-Link無線路由器部分型號存在隱藏功能，攻擊者發送特定封包至網頁服務後可強制啟用telnet服務，並用hard-coded帳號通行碼進行登入與操作。透過此方式開啟的telnet服務必須與設備在同一區域網才能存取。
解決方法	更新DIR-X4860 A1韌體至1.04B05(含)以後版本 更新COVR-X1870韌體至1.03B01(含)以後版本
公開日期	2024-09-16
相關連結	https://www.twcert.org.tw/tw/cp-132-8086-93ed5-1.html

D-Link 無線路由器 - Hidden Functionality	
TVN / CVE ID	TVN-202409024 / CVE-2024-45697
CVSS	9.8 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

影響產品	DIR-X4860 A1 韌體 1.00, 1.04 版本
問題描述	D-Link無線路由器部分型號存在隱藏功能，於WAN port插線的情況下telnet服務會被強制啟用，未經身分鑑別之遠端攻擊者可利用hard-coded帳號通行碼進行登入並執行OS指令。
解決方法	更新DIR-X4860 A1韌體至1.04B05(含)以後版本
公開日期	2024-09-16
相關連結	**https://www.twcert.org.tw/tw/cp-132-8088-590ed-1.html**

D-Link 無線路由器 - OS Command Injection	
TVN / CVE ID	TVN-202409025 / CVE-2024-45698
CVSS	8.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	DIR-X4860 A1 韌體 1.00, 1.04 版本
問題描述	D-Link無線路由器部分型號之telnet服務未妥善驗證使用者輸入，允許未經身分鑑別之遠端攻擊者利用Hard-Coded帳號通行碼登入telnet後，可注入任意OS指令並於設備上執行。
解決方法	更新DIR-X4860 A1韌體至1.04B05(含)以後版本
公開日期	2024-09-16
相關連結	**https://www.twcert.org.tw/tw/cp-132-8090-bf06b-1.html**

D-Link 無線路由器 - OS Command Injection

TVN / CVE ID	TVN-202409025 / CVE-2024-45698
CVSS	8.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	DIR-X4860 A1 韌體 1.00, 1.04 版本
問題描述	D-Link無線路由器部分型號之telnet服務未妥善驗證使用者輸入，允許未經身分鑑別之遠端攻擊者利用Hard-Coded帳號通行碼登入telnet後，可注入任意OS指令並於設備上執行。
解決方法	更新DIR-X4860 A1韌體至1.04B05(含)以後版本
公開日期	2024-09-16
相關連結	**https://www.twcert.org.tw/tw/cp-132-8090-bf06b-1.html**

普萊德科技交換器設備 - Remote privilege escalation using hard-coded credentials	
TVN / CVE ID	TVN-202409004 / CVE-2024-8448
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	GS-4210-24PL4C hardware 2.0 GS-4210-24P2S hardware 3.0
問題描述	普萊德科技部分交換器型號之特定命令列介面存在hard-coded帳號通行碼，已取得一般權限之遠端攻擊者以該組帳密登入後可取得Linux root shell。
解決方法	更新 GS-4210-24PL4C hardware 2.0 之韌體至 2.305b240719(含)以後版本 更新 GS-4210-24P2S hardware 3.0 之韌體至 3.305b240802(含)以後版本

公開日期	2024-09-30
相關連結	**https://www.twcert.org.tw/tw/cp-132-8045-a2804-1.html**

普萊德科技交換器設備 - Hard-coded SNMPv1 read-write community string	
TVN / CVE ID	TVN-202409006 / CVE-2024-8450
CVSS	8.6 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H
影響產品	GS-4210-24PL4C hardware 2.0 GS-4210-24P2S hardware 3.0
問題描述	普萊德科技部分交換器型號之SNMPv1服務存在Hard-coded community string，未經身分鑑別之遠端攻擊者可利用該community string以讀寫權限存取SNMPv1服務。
解決方法	更新 GS-4210-24PL4C hardware 2.0 之韌體至2.305b240719(含)以後版本 更新 GS-4210-24P2S hardware 3.0 之韌體至3.305b240802(含)以後版本
公開日期	2024-09-30
相關連結	**https://www.twcert.org.tw/tw/cp-132-8049-83fe4-1.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9月30 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/**