TWCERT/CC 資安情資電子報

2026 年 8 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

惡意npm攻擊再進化！駭客利用區塊鏈隱藏C2位址

資安社群平臺OpenSourceMalware近期發現兩個遭植入木馬的npm套件「bianira-ui」與「fluid-type-ui」，其攻擊流程不同於傳統的EtherHiding資料隱匿方式，研究人員將這項技術命名為 NullReceiver，並認為此次攻擊可能與北韓駭客組織相關。EtherHiding屬於一種Dead Drop Resolver（DDR）技術，是指攻擊者將惡意中繼站（C2）放置在合

法的第三方平台（如GitHub、Pastebin等），若攻擊者選擇將C2資訊隱藏於區塊鏈上，則被稱為EtherHiding。

「EtherHiding」一詞最早由Guardio Labs於2023年10月提出，Google也在 2025年10月的官方報告中指出，發現國家級攻擊組織開始採用這項手法，並將相關活動歸因於北韓背景的攻擊者。

傳統的EtherHiding手法，通常是將攻擊者欲隱藏的惡意指令或C2寫入區塊鏈交易的 input data欄位中，藉此利用區塊鏈資料的公開性及持久性隱藏惡意內容。這次出現的NullReceiver則採取不同的做法，直接將欲隱藏的資料放在交易的接收者的地址（receiver）地址內，使攻擊者能利用交易地址欄位傳遞攻擊所需資料，進一步增加惡意資訊的辨識及封鎖難度。

研究人員進一步分析 NullReceiver 的運作方式發現，攻擊者錢包（0xA658863Ea658863E68656C6c6f6970626f742121）其中一筆交易紀錄的input data欄位內容為「0x」，並未如傳統EtherHiding手法於該欄位存放惡意資訊（如圖1），進一步檢視該筆交易後，該筆交易真正傳遞的是接收者地址，將這組目標地址進行解碼後，即可解析出攻擊者惡意中繼站的IP位址為166[.]88.134.62，如圖2所示。也就是說，NullReceiver不再把C2藏在容易被注意到的交易資料欄位，而是直接利用區塊鏈交易中的接收者地址承載資訊，降低惡意資訊直接出現在交易資料欄位的特徵，增加防禦端辨識及追蹤相關基礎設施的難度。

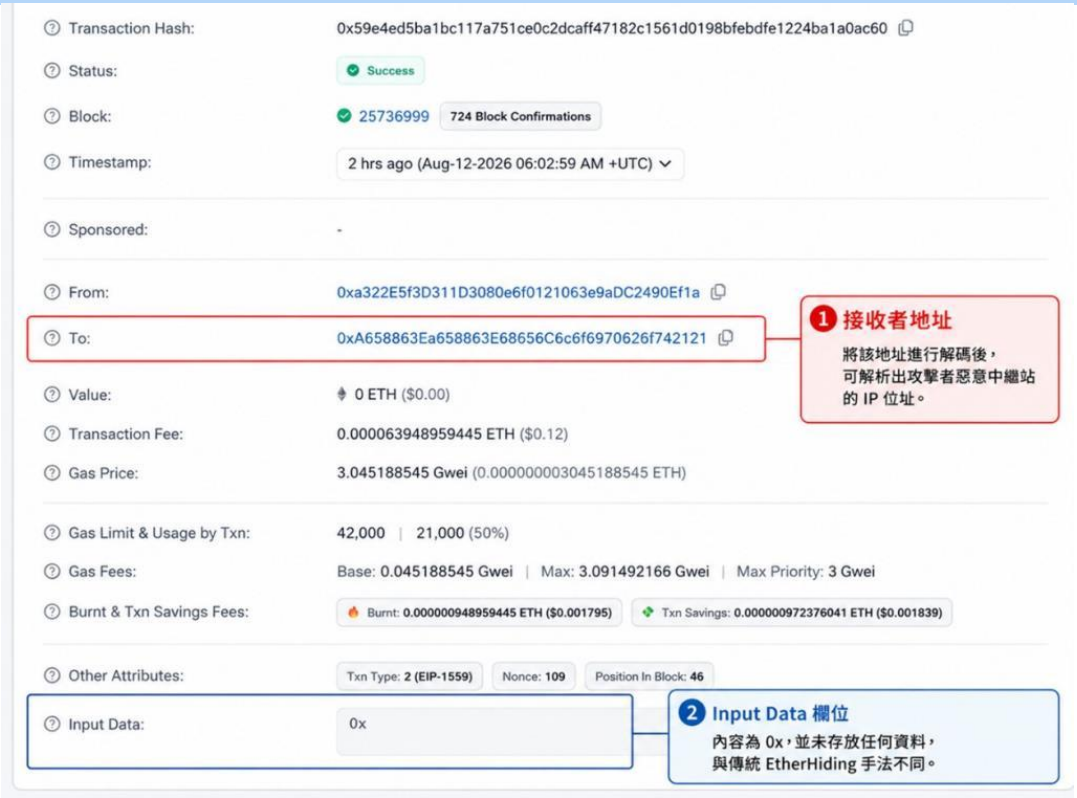

圖1：攻擊者錢包的交易紀錄分析。資料來源：TWCERT/CC整理

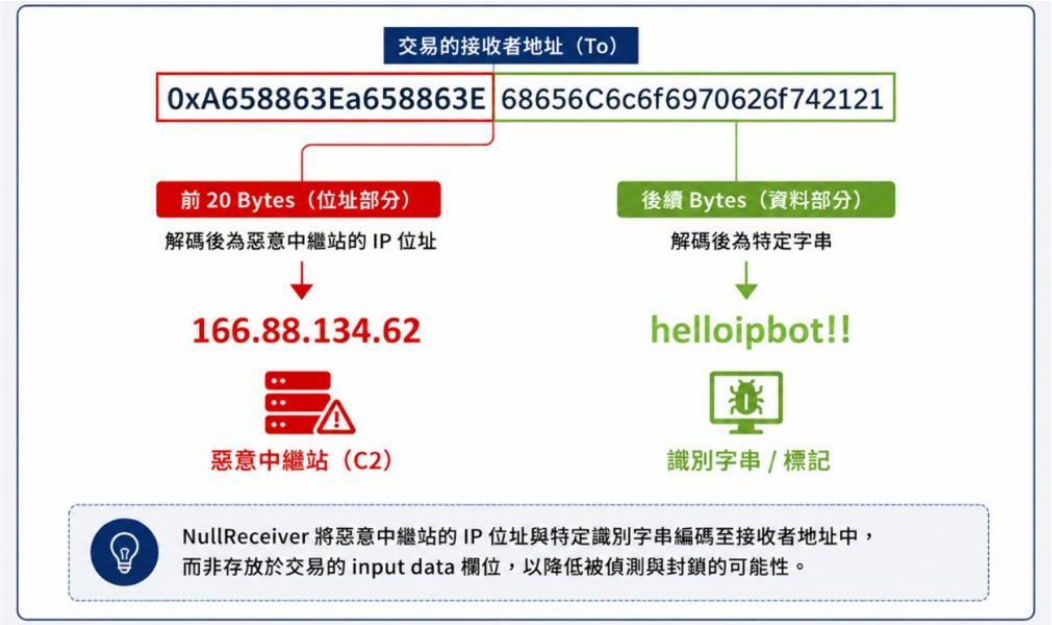

圖2：目標地址解碼與C2分析。資料來源：TWCERT/CC整理

NullReceiver 與傳統 EtherHiding 的差異，不僅在於惡意資訊的藏匿位置，也涉及攻擊者更新惡意資訊時的交易成本。過去攻擊者會將惡意指令寫入區塊鏈交易的input data，根據Google資安人員分析，每次更新惡意指令的成本約為1至2美元；而NullReceiver改變資料藏匿的位置，將資訊編碼至交易的接收者地址，並透過一般以太坊交易將資料寫入鏈上。依據以太坊（Ethereum）的交易機制，任何一筆基本交易的最低固定成本為21,000 Gas（換算約1美元），這是以太坊協議所規定的最低門檻。相較於寫入input data需隨資料量增加Gas費用的做法，NullReceiver能進一步將更新惡意指令的開銷降至最低。

更值得關注的是，NullReceiver並非僅應用在單一npm套件，根據資安社群平臺OpenSourceMalware截至2026年8月12日的最新情資，已累積發現15個npm套件採用NullReceiver攻擊手法。若需查詢遭判定為惡意且使用該技術的完整套件清單，可參閱OpenSourceMalware所整理的相關紀錄：OpenSourceMalware Community-driven threat intel

從此次事件可見，EtherHiding的攻擊手法仍在持續進化。NullReceiver 不僅改變藏匿方式，更試圖降低攻擊者的維運成本。當區塊鏈從交易工具變成惡意基礎設施的藏身處，也代表供應鏈攻擊的威脅追蹤與安全防禦，正面臨更嚴峻的挑戰。本次資安事件之重要威脅指標（IOC）如下：

IOC類型	IOC值
攻擊者錢包地址	0xa322e5f3d311d3080e6f0121063e9adc2490ef1a
惡意中繼站 IP	166[.]88.134.62

- 相關連結
  1. Trojanized npm Packages Employ NullReceiver Tactic to Decode C2 IP from Blockchain
  2. Etherhide Explained: The Rise of Blockchain-Based Command and Control
  3. “EtherHiding” Hiding Web2 Malicious Code in Web3 Smart Contracts
  4. NullReceiver's Blank Crypto Transfers Solves the Challenges of EtherHiding

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 CRA強化軟體供應鏈安全要求，SBOM成企業重要管理工具

隨著歐盟《網路韌性法》（Cyber Resilience Act, CRA）相關規範陸續上路，SBOM（Software Bill of Materials，軟體物料清單）逐漸從最佳實踐（best practice）成為企業因應法規及市場要求的重要管理措施。對於產品涉及數位元件並銷往歐盟市場的業者而言，如何建立、維護及管理SBOM，已成為軟體供應鏈安全的重要課題。

SBOM實務導入涉及軟體範圍、元件盤點、資料格式、更新機制及

維護責任等多項管理議題。企業除應掌握SBOM的基本概念外，亦需建立適當的產製及管理流程，以確保軟體元件資訊具備完整性、可追溯性及可持續維護性。

SBOM是什麼

SBOM是一份正式且機器可讀性的軟體元件清單，用於記錄軟體所使用的元件（component）、函式庫（library）及相依套件（dependency），以及相關版本、供應來源與相依關係等。透過SBOM，企業可掌握軟體產品的組成，並進一步建立軟體元件與供應鏈之間的關聯性。

SBOM的核心價值主要在於四項能力—透明度（Transparency）、可追溯性（Traceability）、合規（Compliance）、安全（Security）。

- 透明度：掌握軟體產品所使用的第三方與開源元件，降低因缺乏元件清單而無法確認軟體組成的情形。
- 可追溯性：建立軟體元件與上游供應商、產品及下游使用情境之間的關聯，一旦某個元件被發現安全有漏洞，才能快速鎖定哪些系統會受影響，不用整批盤點。
- 合規：提供企業進行法規、客戶要求及供應鏈安全管理時的佐證資料，，協助確認軟體組成及相關管理措施。
- 安全：將SBOM的元件清單與弱點情資進行比對，及早抓出已知漏洞影響的產品或系統，並支援後續風險評估與處置。

對企業來說，SBOM不只是提供軟體元件清單，而是作為軟體供應鏈風險管理的重要基礎資料。當軟體元件出現安全漏洞或供應鏈事件時，企業可透過SBOM快速確認受影響範圍，縮短盤點及應變所需時間。

CRA對SBOM的要求

CRA針對具有數位元素的產品（products with digital elements）建立網路安全要求，並要求製造商建立並維護相關技術文件及軟體物料清單。SBOM應涵蓋產品中至少最上層的相依性（top-level dependencies），並採用常用且機器可讀的格式，以支援軟體組成資訊的管理及後續安全分析。

不過，法規所提出的要求主要著重於必要條件，企業實際導入SBOM時，仍須進一步處理元件盤點範圍、產製方式、資料格式、更新頻率、責任分工及維護機制等執行層面的問題。因此，企業除確認是否建立SBOM外，亦應確保其內容能夠反映實際軟體組成，並建立持續更新及管理機制。

官方資源提供導入參考

ENISA 在 2025 年 12 月 17 日發布《SBOM Landscape Analysis – Towards an Implementation Guide》公開草案並展開意見徵集，內容針對企業導入SBOM的流程及實務作法提供參考，草案提及企業導入SBOM區分為五個階段：啟動、規劃、執行、監控、結案等，並針對每個階段給出具體的操作建議，可作為企業規劃SBOM管理機制的參考。

ENISA草案可作為SBOM的規劃面參考，而國家資通安全研究院的《SBOM開源工具使用說明》，則示範怎麼用Syft、Trivy這類開源工具替專案掃描產生SBOM檔案，再串接Google的OSV開源漏洞資料庫，企業可依自身軟體開發及供應鏈管理需求，參考相關工具及作法建立SBOM產製、分析及管理流程。

對企業而言，SBOM的導入重點不僅在於「建立一份清單」，更在於確保清單內容能持續反映軟體實際組成，並可與漏洞管理及資安事件

應變機制相互連結。透過建立完整的軟體元件可視性，企業可在面對新興漏洞或供應鏈資安事件時，更快速掌握受影響範圍並採取適當處置措施。

- 相關連結
  1. SBOM LANDSCAPE ANALYSIS
  2. Call for Feedback: Advancing Software Supply Chain Security together!
  3. 國家資通安全研究院（NICS）。（2026年3月25日更新）。SBOM開源工具使用說明。
  4. TWCERT/CC. (2026, July 29). SBOM做了，為什麼還可能不合規？ENISA調查揭露近三成企業用錯

2.2 國際政府組織資安資訊

2.2.1 CISA與多國安全機構聯合發布「Gunra」勒索軟體預警通報

網路安全威脅持續升溫，名為「Gunra」的勒索軟體即服務（Ransomware-as-a-Service）自2025 年 4 月首次被發現後，相關攻擊活動持受到國際資安與執法機構關注。Gunra採用「雙重勒索（Double Extortion）」模式，除加密受害組織檔案外，亦會於加密前竊取資料，並以公開或洩露遭竊資料作為談判籌碼，增加受害組織的營運及資料外洩風險。

美國網路安全暨基礎設施安全局（CISA）、聯邦調查局（FBI）及國

家安全局（NSA）等多個跨國安全與執法機構聯合發布詳細的資安警報，指出勒索軟體攻擊已持續鎖定醫療、金融、政府、公共設施及學術機構等不同領域組織。對企業而言，Gunra 所呈現的攻擊模式並非僅限於惡意程式本身，而是結合網路邊界設備漏洞、帳號及憑證濫用、遠端存取服務及內部環境偵察等手法，值得相關單位提高警覺。

從已公開的攻擊活動觀察，Gunra 攻擊者在初始存取階段，除可能透過偽冒微軟安全驗證等內容進行網路釣魚外，也會鎖定對外暴露的網路邊緣設備，例如 Fortinet FortiOS 和 FortiProxy 的 CVE-2024-55591(CVSS:9.8) 與 CVE-2025-24472(CVSS:8.1)等身分驗證繞過漏洞。若相關設備存在漏洞且未完成修補，攻擊者可能藉此取得未經授權的存取權限，進一步作為後續攻擊的切入點。

取得初始權限後，攻擊者在進行檔案加密前，先竊取受害者的內部機敏文件、並匯出管理人員的虛擬桌面（VDI）環境的設置檔；隨後再啟動加密程式，將受害者電腦中的檔案副檔名更改為「.ENCRT」。當受害者系統遭到鎖定後，所有加密的資料夾內皆會留下檔名為「R3ADM3.txt」的勒索說明檔，Gunra組織通常在勒索信件中要求受害者於限定期限內回應，否則將面臨資料永久毀損或機敏檔案於資料洩露網站公開兜售的風險，形成資料外洩與營運中斷的雙重風險，Gunra攻擊流程請參考表1。

攻擊階段	檢視重點
初始入侵	邊界設備漏洞、VPN、SSH、網路釣魚
權限取得	管理員帳號、預設帳號、異常權限變更
內部偵查	AD、VDI、內部網路及帳號活動
資料竊取	大量檔案存取、異常資料傳輸

表1：Gunra攻擊流程表。資料來源：TWCERT/CC整理

除了邊緣設備漏洞外，也觀察到攻擊者透過VPN閘道憑證外洩，SSH的存取控制漏洞及取得未經授權的遠端存取權限，從而進行初步入侵。在部分案例中，攻擊者利用預設憑證直接取得 SSL-VPN 設備的管理員權限，進而修改未使用帳號的設定，以避開強制變更密碼機制，藉此在受害網域中長期潛伏。此外，Gunra 攻擊者主要利用深夜與凌晨時段進行惡意活動與內部基礎設施的偵察，並透過清除系統日誌檔（Log）與命令歷史紀錄等手法規避資安人員偵測。

根據 Gunra 的攻擊手法，建議企業與組織實施以下緩解措施：

1. 優先修補對外服務與邊界設備漏洞：優先檢視對外服務的系統與設備，包含VPN閘道器、防火牆及遠端桌面 RDP，確認作業系統、應用程式及設備韌體隨時維持在最新版本，避免成為攻擊者首選的突破口。
2. 落實離線與不可篡改備份：平時應定期備份重要資料，且備份檔案必須儲存在與主要網路實體隔離、劃分獨立網段的安全空間中，並確保其具備「不可篡改」屬性。
3. 實施網段隔離：依系統功能及資料重要性進行網路分區，限制不同網段及系統間不必要的連線，並妥善控管伺服器、NAS、VDI等重要資源的存取權限，降低單一端點遭入侵後，攻擊者進一步進行橫向移動及擴大影響範圍的風險。
4. 啟用多因子驗證（MFA）：對於 VPN、企業電子郵件及關鍵帳戶全面強制啟用MFA，並定期清查預設、停用及長期未使用的帳號，移除不必要的存取權限。另應注意 MFA 並非萬無一失，仍須防範憑證及 Session Token 遭竊取，以及釣魚等方式繞過驗證機制。

5. 強化異常活動監控與事件應變能力：建立 VPN、邊界設備、AD、伺服器及端點等重要系統的日誌蒐集與監控機制，特別留意異常登入、管理員權限變更、大量檔案存取、異常資料傳輸及可疑的日誌清除行為。若發現不明的遠端登入或管理操作，應立即進行帳號、端點及網路連線調查，以降低攻擊者長時間潛伏及資料竊取的風險。

提供企業與組織防範此資安威脅，以下整理多個國際資安機構與研究報告所釋出之 Gunra 勒索軟體相關惡意指標如下：

類型	IoC
MD5	7dd26568049fac1b87f676ecfaac9ba0
MD5	9a7c0adedc4c68760e49274700218507
MD5	ae6f61c0fc092233abf666643d88d0f3
MD5	f6664f4e77b7bcc59772cd359fdf271c
SHA1	bb79502d301ba77745b7dbc5df4269fc7b074cda
SHA1	0c3c878b678c7254446e84cca6f0d63caeb51880
SHA1	77b294117cb818df701f03dc8be39ed9a361a038
SHA1	be6ee00fa5284ee4237f877f4bd5cfa871fdc6ef
SHA1	79e19d3d8405425735e4b3cd36a8507d99dfee20
SHA1	912217b09b13e1e53f7f26335f7f84b3c3918491
SHA1	8404521cf2a53de3459a75ff946873c43211afb6
SHA256	2dc70a12d158d437e45a55b1d52f3d61c6082a1e1667573302ba3b62813e2751
SHA256	834efe9b392c6c000877ea5613a079445affc16fe8af5997d68c55cafc95e5d1
SHA256	91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0
SHA256	a82e496b7b5279cb6b93393ec167dd3f50aff1557366784b25f9e51cb23689d9
IP	86[.]54.28.216

- 相關連結

1. CISA - #StopRansomware: Gunra Ransomware
2. Gunra Ransomware Exploits Fortinet FortiOS, FortiProxy Flaws to Breach Networks
3. GUNRA RANSOMWARE: What You Don't Know!
4. Gunra Ransomware Group Unveils Efficient Linux Variant
5. Gunra Ransomware – A Brief Analysis

2.3 軟硬體漏洞資訊

2.3.1 Microsoft Excel存在高風險安全漏洞(CVE-2026-62870)，請儘速確認並進行修補

CVE 編號	CVE-2026-62870
影響產品	Microsoft 365 Apps for Enterprise、Microsoft Excel 2016、Microsoft Office 2019、Microsoft Office LTSC 2021、Microsoft Office LTSC 2024
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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62870

- 內容說明：

  研究人員發現 Microsoft Excel 存在使用釋放後記憶體(Use After Free)漏洞(CVE-2026-62870)，未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - Microsoft 365 Apps for Enterprise for 32-bit Systems
  - Microsoft 365 Apps for Enterprise for 64-bit Systems
  - Microsoft Excel 2016 (32-bit edition) 16.0.5561.1001(不含)以前版本
  - Microsoft Excel 2016 (64-bit edition) 16.0.5561.1001(不含)以前版本
  - Microsoft Office 2019 for 32-bit editions
  - Microsoft Office 2019 for 64-bit editions
  - Microsoft Office LTSC 2021 for 32-bit editions
  - Microsoft Office LTSC 2021 for 64-bit editions
  - Microsoft Office LTSC 2024 for 32-bit editions
  - Microsoft Office LTSC 2024 for 64-bit editions

- 資料來源：
  1. CVE-2026-62870
  2. Microsoft Excel 遠端執行程式碼弱點

2.3.2 Cisco旗下Integrated Management Controller 存在重大資安漏洞(CVE-2026-20200)

CVE 編號	CVE-2026-20200
影響產品	Cisco Integrated Management Controller
解決辦法	根據官方網站釋出的解決方式進行修補： https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-arg-inject-upSHdMfU

- 內容說明：

  Cisco 旗下整合管理控制器(Integrated Management Controller，IMC)是一款專門為 Cisco 整合運算系統的伺服器設計管理工具，提供伺服器遠端監控、配置和管理功能。近日 Cisco 發布重大資安公告(CVE-2026-20200，CVSS：8.8)，該漏洞允許經身分驗證的遠端攻擊者可能在受影響的底層作業系統上，執行任意程式碼或命令，並將權限提升至 root。

- 影響平台：
  - UCS C-Series M7 and M8 Rack Servers in standalone mode
- 資料來源：
  1. Cisco Integrated Management Controller Argument Injection Vulnerabilities
  2. CVE-2026-20200

2.3.3 Cisco旗下 IOS XE Software 存在2個重大資安漏洞

CVE 編號	CVE-2026-20267,CVE-2026-20272
影響產品	Cisco IOS XE
解決辦法	請更新至以下版本： Cisco IOS XE 17.12.18(含)之後版本、 Cisco IOS XE 17.15.6(含)之後版本、 Cisco IOS XE 17.18.4(含)之後版本、 Cisco IOS XE 17.18.4a(含)之後版本、 Cisco IOS XE 26.1.2(含)之後版本

- 內容說明：

  Cisco IOS XE 軟體開發團隊於內部安全審查期間發現多項安全漏洞，並已完成修補。目前尚未發現有證據顯示這些漏洞遭到積極利用。為協助客戶及時部署安全更新並簡化漏洞揭露流程，Cisco 已公開相關漏洞資訊及修補建議。CVE-2026-20267(CVSS：9.0)為存取控制不當漏洞；CVE-2026-20272(CVSS：9.8)為特殊元素未適當處理漏洞。

- 影響平台：
  - Cisco IOS XE 17.9 版本
  - Cisco IOS XE 17.12 版本
  - Cisco IOS XE 17.15 版本
  - Cisco IOS XE 17.18 版本
  - Cisco IOS XE 26.1 版本
- 資料來源：
  1. Cisco IOS XE Software Security Hardening Release: August 2026
  2. CVE-2026-20267
  3. CVE-2026-20272

2.3.4 Cisco Catalyst SD-WAN 存在4個重大資安漏洞

CVE 編號	CVE-2026-20303,CVE-2026-20304,CVE-2026-20310,CVE-2026-20312
影響產品	Cisco Catalyst SD-WAN
解決辦法	請更新至以下版本： Cisco Catalyst SD-WAN 20.9.10(含)之後版本、 Cisco Catalyst SD-WAN 20.12.8.1(含)之後版本、 Cisco Catalyst SD-WAN 20.15.6(含)之後版本、 Cisco Catalyst SD-WAN 20.18.4(含)之後版本、 Cisco Catalyst SD-WAN 26.1.2(含)之後版本

- 內容說明：

  Cisco Catalyst SD-WAN 是 Cisco 以雲端為中心的軟體定義廣域網路架構，提供集中管理、安全加密及應用效能優化，確保多雲環境的可靠連線。Catalyst SD-WAN 軟體開發團隊於內部安全審查期間發現多項安全漏洞，並已完成修補。目前尚未發現有證據顯示這些漏洞遭到積極利用。為協助客戶及時部署安全更新並簡化漏洞揭露流程，Cisco 已公開相關漏洞資訊及修補建議。CVE-2026-20303(CVSS：9.9)為輸入驗證不當漏洞；CVE-2026-20304(CVSS：9.9)為存取控制不當漏洞；CVE-2026-20310(CVSS：9.9)為文件存取前連結解析不正確；CVE-2026-20312(CVSS：8.8)為以明文形式儲存敏感資訊。

- 影響平台：
  - Cisco Catalyst SD-WAN 20.9(含)之前版本
  - Cisco Catalyst SD-WAN 20.10 版本
  - Cisco Catalyst SD-WAN 20.11 版本
  - Cisco Catalyst SD-WAN 20.12 版本
  - Cisco Catalyst SD-WAN 20.13 版本

- Cisco Catalyst SD-WAN 20.14 版本
- Cisco Catalyst SD-WAN 20.15 版本
- Cisco Catalyst SD-WAN 20.16 版本
- Cisco Catalyst SD-WAN 20.18 版本
- Cisco Catalyst SD-WAN 26.1 版本

- 資料來源：
  1. Cisco Catalyst SD-WAN Software Security Hardening Release: August 2026
  2. CVE-2026-20303
  3. CVE-2026-20304
  4. CVE-2026-20310
  5. CVE-2026-20312

2.3.5 Veeam Service Provider Console 存在2個重大資安漏洞

CVE 編號	CVE-2026-58073,CVE-2026-58072
影響產品	Veeam Service Provider Console
解決辦法	請將 Veeam Service Provider Console 更新至 9.3.0.35057 (含)之後版本

- 內容說明：

  備份與資料保護軟體廠商 Veeam 旗下遠端管理控制臺(Veeam Service Provider Console ，VSPC)是一款用於跨本地雲端應用環境的遠端監控與管理工具，日前官方提修補高風險資安漏洞(CVE-2026-58073，CVSS 4.x：9.5 和 CVE-2026-58072，CVSS 4.x：9.0)。CVE-2026-58073 允許未經身分驗證的攻擊者，冒充受管代理程式並取得該憑證；CVE-2026-58072 允許對管理伺服器進行任意檔案寫入，可能導致遠端程式碼執行。

- 影響平台：
  - Veeam Service Provider Console 9 版本
  - Veeam Service Provider Console 9.2.1.33875
- 資料來源：
  1. Vulnerabilities Resolved in Veeam Service Provider Console 9.3
  2. CVE-2026-58073
  3. CVE-2026-58072

2.3.6 cPanel 與 WHM (WebHost Manager) 存在重大資安漏洞(CVE-2026-58048)

CVE 編號	CVE-2026-58048
影響產品	cPanel/WHM
解決辦法	請更新至以下版本： cPanel/WHM 11.110.0.137 版本、 cPanel/WHM 11.118.0.71 版本、 cPanel/WHM 11.126.0.78 版本、 cPanel/WHM 11.134.0.48 版本、 cPanel/WHM 11.136.0.32 版本、 cPanel/WHM 138.1.6 (WP2)版本

- 內容說明：

  近日 cPanel 發布重大資安公告(CVE-2026-58048，CVSS 4.x：9.4)，此漏洞存在於 cPanel 與 WHM（WebHost Manager） 管理系統中，屬於權限提升漏洞。已通過身分驗證且具有 MySQL/MariaDB 資料庫存取權限的 cPanel 帳戶，可能利用此漏洞執行任意資料庫指令的完全管理權限。

- 影響平台：
  - cPanel 與 WHM (WebHost Manager) 所有版本
- 資料來源：
  1. Security: CVE-2026-58048 Database Privilege Escalation
  2. CVE-2026-58048

2.3.7 pgAdmin 4存在高風險安全漏洞(CVE-2026-17566)，請儘速確認並進行修補

CVE 編號	CVE-2026-17566
影響產品	pgAdmin 4
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://www.postgresql.org/about/news/pgadmin-4-v917-released-3356/

- 內容說明：

  研究人員發現 pgAdmin 4 存在作業系統指令注入(OS Command Injection)高風險安全漏洞(CVE-2026-17566)。由於 pgAdmin 4 之資料匯入/匯出工具(Import/Export Data)未妥善處理 SQL 查詢，已通過身分鑑別之遠端攻擊者，可利用此漏洞執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - pgAdmin 4 之 1.0 至 9.16 版本
- 資料來源：
  1. CVE-2026-17566
  2. pgAdmin 4 v9.17 Released

2.3.8 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2026-58231,CVE-2026-34265,CVE-2026-44758,CVE-2026-58243
影響產品	SAP Commerce Cloud、NetWeaver and ABAP Platform、Manufacturing Integration and Intelligence、ABAP Developer Tools
解決辦法	根據官方網站釋出的解決方式進行修補：https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2026.html?isu_page=1

- 內容說明：

  SAP 發布八月份例行更新，其中 4 項屬於高風險資安漏洞。

  【CVE-2026-58231，CVSS：10.0】

  SAP Commerce Cloud 允許未經身分驗證的攻擊者濫用預設身分驗證用戶端，向某些缺乏完整驗證的函數提交精心設計的輸入，若成功利用此漏洞可能導致任意程式碼執行並破壞內部元件。

  【CVE-2026-34265，CVSS：9.8】

  SAP NetWeaver and ABAP Platform 允許未經身分驗證的攻擊者可利用 DIAG 協定解析中的邏輯錯誤，可能導致記憶體損壞、洩漏敏感系統資訊或系統崩潰。

  【CVE-2026-44758，CVSS：9.1】

  SAP Manufacturing Integration and Intelligence 允許具有高權限的攻擊者向某些受影響的功能提交精心設計的輸入，在未經充分驗證的情況下，若攻擊者功能利用此漏洞可在底層作業系統上執行任意命令。

  【CVE-2026-58243，CVSS：8.8】

  SAP ABAP Developer Tools 的某些功能未執行必要的授權檢查，導致權限較低的攻擊者可對 SAP NetWeaver AS ABAP 執行未經授權的資

料庫操作，若成功利用此漏洞可能導致攻擊者讀取敏感資料、修改應用程式資料並中斷合法用戶訪問。

- 影響平台：
  - SAP Commerce Cloud (Data Hub Adapter)
    Version(s) - COM_CLOUD 2211, 2211-JDK21
  - SAP NetWeaver and ABAP Platform
    Version(s) - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.22EXT2, 7.22EXT3, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.16 9.18, 9.19, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.16, 9.18, 9.19
  - SAP Manufacturing Integration and Intelligence
    Version(s) - XMII 15.4, 15.5
  - SAP ABAP Developer Tools
    Version(s) - 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 816, SAP_BASIS 918, SAP_BASIS 920
- 資料來源：
  1. SAP Security Patch Day - August 2026
  2. CVE-2026-58231
  3. CVE-2026-34265
  4. CVE-2026-44758
  5. CVE-2026-58243

2.3.9 SonicWall GMS 存在2個重大資安漏洞

CVE 編號	CVE-2026-66145,CVE-2026-66147
影響產品	SonicWall GMS
解決辦法	請將 SonicWall GMS 更新至 9.5.2(含)之後版本

- 內容說明：

  SonicWall 針對旗下產品 GMS 發布重大資安漏洞公告 (CVE-2026-66145，CVSS：9.1 與 CVE-2026-66147，CVSS：9.4)。CVE-2026-66145 為未經身分驗證的遠端程式碼執行漏洞，允許遠端攻擊者透過 zipslip 讀取敏感資料並執行任意檔案寫入；CVE-2026-66147 為未經身分驗證的命令注入漏洞，允許遠端攻擊者可透過精心設計的請求執行遠端程式碼。

- 影響平台：
  - SonicWall GMS 9.5.1(含)之前版本
- 資料來源：
  1. SonicWall GMS Security Affected By Multiple Vulnerabilities
  2. CVE-2026-66145
  3. CVE-2026-66147

2.3.10 Fortinet旗下FortiWeb存在重大資安漏洞(CVE-2026-26035)

CVE 編號	CVE-2026-26035
影響產品	FortiWeb
解決辦法	請更新至以下版本： FortiWeb 7.2.13 版本(含)之後版本、 FortiWeb 7.4.12 版本(含)之後版本、 FortiWeb 7.6.7 版本(含)之後版本、 FortiWeb 8.0.3 版本(含)之後版本

- 內容說明：

  Fortinet 旗下 FortiWeb 是一款提供網站應用程式的防火牆產品，其功能涵蓋異常偵測、API 保護、機器人緩解和進階威脅分析等。日前，Fortinet 發布重大資安漏洞公告(CVE-2026-26035，CVSS：9.8)，FortiWeb 遠端 Radius 類型管理員身分驗證配置中存在身分驗證不當漏洞，使用特定的非預設設定時，可能允許未經身分驗證的遠端攻擊者，使用隨機使用者名稱和密碼登入 FortiWeb GUI/CLI。

- 影響平台：
  - FortiWeb 7.2.0 至 7.2.12 版本
  - FortiWeb 7.4.0 至 7.4.11 版本
  - FortiWeb 7.6.0 至 7.6.6 版本
  - FortiWeb 8.0.0 至 8.0.2 版本
- 資料來源：
  1. Broken access control in the RADIUS type admin group
  2. CVE-2026-26035

2.3.11 Oracle針對旗下多款產品發布重大資安公告

CVE 編號	詳見附件說明
影響產品	詳見附件說明
解決辦法	根據官方網站釋出的解決方式進行修補： https://www.oracle.com/security-s/cspuaug2026.html

- 內容說明：

  Oracle 近期釋出 115 年 8 月關鍵安全性修補程式更新公告，包含多個重大安全漏洞，請儘速確認並進行修補。(詳見附件說明)

- 影響平台：
  - 詳見附件說明
- 資料來源：
  1. Oracle Critical Security Patch Update Advisory - August 2026

2.3.12 Cisco旗下Cisco Crosswork 存在4個重大資安漏洞

CVE 編號	CVE-2026-20030,CVE-2026-20357,CVE-2026-20358,CVE-2026-20359
影響產品	Cisco Crosswork
解決辦法	請更新至 Cisco Crosswork 7.2.1-SP(含)之後版本

- 內容說明：

  Cisco Crosswork 開發團隊於內部安全審查期間發現多項安全漏洞，並已完成修補。目前尚未發現有證據顯示這些漏洞遭到積極利用。為協助客戶及時部署安全更新並簡化漏洞揭露流程，Cisco 已公開相關漏洞資訊及修補建議。CVE-2026-20030(CVSS：10.0)為 SQL 指令所使用的特殊元素未適當處理漏洞；CVE-2026-20357(CVSS：10.0)為關鍵功能缺少身分驗證漏洞；CVE-2026-20358(CVSS：10.0)為外部控制檔案名稱或路徑漏洞；CVE-2026-20359(CVSS：9.8)為憑證保護不足漏洞。

- 影響平台：
  - Cisco Crosswork 7.2.1(含)以前版本
- 資料來源：
  1. Cisco Crosswork Security Hardening Release: August 2026
  2. CVE-2026-20030
  3. CVE-2026-20357
  4. CVE-2026-20358
  5. CVE-2026-20359

2.3.13 Cisco Secure Workload 存在4個重大資安漏洞

CVE 編號	CVE-2026-20231,CVE-2026-20315,CVE-2026-20317,CVE-2026-20318
影響產品	Cisco Secure Workload
解決辦法	請更新至以下版本： Cisco Secure Workload 3.10.9.1(含)之後版本、 Cisco Secure Workload 4.0.4.16(含)之後版本

- 內容說明：

  Cisco Secure Workload 開發團隊於內部安全審查期間發現多項安全漏洞，並已完成修補。目前尚未發現有證據顯示這些漏洞遭到積極利用。為協助客戶及時部署安全更新並簡化漏洞揭露流程，Cisco 已公開相關漏洞資訊及修補建議。CVE-2026-20231(CVSS：9.9)為特殊元素未適當處理漏洞；CVE-2026-20315(CVSS：10.0)為存取控制不當漏洞；CVE-2026-20317(CVSS：10.0)為身分驗證不當漏洞；CVE-2026-20318(CVSS：9.6)為輸入驗證不當漏洞。

- 影響平台：
  - Cisco Secure Workload 3.10(含)以前版本
  - Cisco Secure Workload 4.0 版本
- 資料來源：
  1. Cisco Secure Workload Software Security Hardening Release: August 2026
  2. CVE-2026-20231
  3. CVE-2026-20315
  4. CVE-2026-20317
  5. CVE-2026-20318

2.3.14 NetScaler ADC與NetScaler Gateway存在2個重大資安漏洞

CVE 編號	CVE-2026-19489,CVE-2026-19490
影響產品	NetScaler ADC & NetScaler Gateway、NetScaler ADC FIPS、NetScaler ADC FIPS & NDcPP
解決辦法	請更新至以下版本： NetScaler ADC 和 NetScaler Gateway 14.1-73.32 (含)之後版本、 NetScaler ADC 和 NetScaler Gateway 13.1-63.21 (含)之後版本、 NetScaler ADC FIPS 14.1-73.32(含)之後版本、 NetScaler ADC FIPS 與 NDcPP 13.1-37.277(含)之後版本

- 內容說明：

  Citrix 旗下 NetScaler ADC (原名為 Citrix ADC)是一款網路設備，專為優化、保護及管理企業應用程式與雲端服務而設計；NetScaler Gateway (原名為 Citrix Gateway)則提供安全的遠端存取解決方案，讓使用者能夠從任何地點安全存取應用程式和資料。近日，Citrix 發布重大資安漏洞公告(CVE-2026-19489，CVSS 4.x：8.8、CVE-2026-19490，CVSS 4.x：9.3)，CVE-2026-19489，為記憶體溢出漏洞，可能導致不可預測的行為或 DoS 攻擊；CVE-2026-19490，允許遠端攻擊者在無須互動或提升權限的情況下，直接繞過網路身分驗證。

- 影響平台：
  - NetScaler ADC 與 NetScaler Gateway 14.1 至 14.1-73.32(不含)版本
  - NetScaler ADC 與 NetScaler Gateway 13.1 至 13.1-63.21(不含)版本
  - NetScaler ADC FIPS 14.1-73.32(不含)以前版本
  - NetScaler ADC FIPS 與 NDcPP 13.1-37.277(不含)以前版本

- 資料來源：
  1. NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2026-19489 and CVE-2026-19490
  2. CVE-2026-19489
  3. CVE-2026-19490

2.3.15 SonicWall NetExtender Linux存在重大資安漏洞(CVE-2026-66152)

CVE 編號	CVE-2026-66152
影響產品	SonicWall NetExtender Linux
解決辦法	請更新至 NetExtender Linux Client 10.3.6(含)之後版本

- 內容說明：

  SonicWall 針對旗下產品 SonicWall NetExtender Linux 發布重大資安漏洞公告 (CVE-2026-66152，CVSS：8.8)，此為路徑遍歷漏洞，攻擊者可以利用該漏洞以 root 身分寫入任意檔案。

- 影響平台：
  - NetExtender Linux Client 10.3.5(含)以前版本
- 資料來源：
  1. SonicWall NetExtender Linux Client Multiple Vulnerabilities 8.8
  2. CVE-2026-66152

2.3.16 Veeam ONE 13.1存在2個重大資安漏洞

CVE 編號	CVE-2026-64633,CVE-2026-65641
影響產品	Veeam ONE
解決辦法	請更新至以下版本： 【CVE-2026-64633】 Veeam ONE 13.1 (build 13.1.0.7034)、 Veeam ONE 13.0.2 Patch 1 (build 13.0.2.7159) 【CVE-2026-65641】 Veeam ONE 13.1 Patch 0 (build 13.1.0.7233) Veeam ONE 13.0.2 Patch 1 (build 13.0.2.7159)

- 內容說明：

  Veeam ONE 是用於監控本地端 Veeam 備份基礎架構。近日，Veeam 發布重大資安漏洞公告(CVE-2026-64633，CVSS 4.x：10.0 和 CVE-2026-65641，CVSS 4.x：9.3)，CVE-2026-64633 允許未經身分驗證的攻擊者在代理主機上遠端執行程式碼；CVE-2026-65641 允許未經身分驗證的攻擊者強制服務帳號進行 SMB 身分驗證。

- 影響平台：
  - Veeam ONE 13.0.2.6723 (含)之前版本
  - Veeam ONE 13.1.0.7034 (含)之前版本
- 資料來源：
  1. Vulnerabilities Resolved in Veeam ONE 13.1
  2. Vulnerability Resolved in Veeam ONE 13.1 Patch 0
  3. CVE-2026-64633
  4. CVE-2026-65641

第 3 章、資安研討會及活動

- **資安研討會**

115年資安事件應變工程師課程_朝陽科技大學（115002期）	
活動時間	115/10/19(一)~115/10/23(五)
活動地點	朝陽科技大學推廣教育處中科分部（臺中市西屯區科園路21號）
活動網站	https://oce.cyut.edu.tw/course/n_course_detail.php?u=acc65ac9182a9a9db8c6b10027ff1621
活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】** 1.第一線保護/回應攻擊之系統管理員或其他安全人員。 2.轉投入資安領域之 IT 技術、系統維護或資訊管理人員。 3.擬投入資安教育之教師。 **【預備知識】** 資通安全概論、網路架構與部署安全。 **【課程目標】**

	具備資安事件應變完整生命週期之基礎知識與各階段之操作技能。 **【師資介紹】許晉銘老師** **【主辦單位】國家資通安全研究院、朝陽科技大學**
115年滲透測試工程師課程_國立中興大學	
活動時間	**115/11/7(六)~115/12/5(六)**
活動地點	**國立中興大學**
活動網站	**https://www.siileec.com/subject.php?sn=6327**
活動概要	 **【費用】** 依各訓練機構收費標準，請參閱報名連結。 **【招生對象】** 系統管理或其他網路安全管理人員、安全事件回應處理相關管理人員、資安技術服務/弱點檢測人員。 **【預備知識】** 基礎資訊技術與資安概、基礎網路安全與 Web、技術分析與邏輯推論能力、風險管理與法律倫理意識。 **【課程目標】** 訓練具備識別資訊系統中的弱點及漏洞，執行漏洞評估、風險分級與管理，提出可行且有效的補救與強化建議報告。 **【師資介紹】徐振煒、李慈偉、許炳昆**

	【主辦單位】國家資通安全研究院、國立中興大學
【資安學院】9/11-資安治理養成術：從風險管控到稽核實戰	
活動時間	**2026-09-11 09:00 ~ 2026-09-11 16:00**
活動地點	**中華軟體公會──大同辦公室D01會議室（ 臺北市中山北路三段22-1號新社工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5893**
活動概要	**【費用】** 原價：7,200元/人 早鳥價：6,800元/人 公會會員：6,000元/人 費用含稅、教材、餐點及完課證明 報名截止：2026-09-08 **【活動內容】** 本課程透過分組討論、情境演練與案例研討等互動式教學，學員將學習如何評估並選擇適切的風險處理措施，以緩解風險發生機率及對組織的衝擊，同時，課程亦強調透過定期稽核或內部自我檢查機制，驗證控制措施的有效性，持續改善與強化組織的資安防護體系，以達成資通安全及個資相關法規的合規要求。 **【主辦單位】中華民國資訊軟體服務商業同業公會** **【聯絡窗口】02-2553-3988#816 林專員** **security@tissa.org.tw**
【資安學院】9/17~9/18-滲透測試與應用實務-實作課	
活動時間	**2026-09-17 09:00 ~ 2026-09-18 17:00**
活動地點	**中華軟體公會──大同辦公室D01會議室（ 臺北市中山北路三段22-1號新社工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5916**
	【費用】

活動概要	原價：12,000元/人 早鳥價：11,000元/人 公會會員：9,500元/人 費用含稅、教材、餐點及完課證明 報名截止：2026-09-15 **【活動內容】** 本課程以實作為核心，說明駭客如何鎖定目標、蒐集資訊、挖掘漏洞並加以利用，進而取得系統控制權，甚至在系統中建立持久性後門，以維持長期滲透。並搭配實作練習，協助學員深度理解弱點形成原因及其危害，同時建立正確的防禦思維，從而能在面對真實威脅時制定有效的資安防禦策略。 **【主辦單位】中華民國資訊軟體服務商業同業公會** **【聯絡窗口】02-2553-3988#816 林專員** **security@tissa.org.tw**
【資安學院】9/22~9/23-AI 上線，駭客下線：智慧防禦的下一步(實作課)	
活動時間	**2026-09-22 09:00 ~ 2026-09-23 16:00**
活動地點	**中華軟體公會──大同辦公室D01會議室（ 臺北市中山北路三段22-1號新社工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5917**
活動概要	**【費用】** 原價：15,000元/人 早鳥價：14,000元/人 公會會員：12,000元/人 費用含稅、教材、餐點及完課證明 報名截止：2026-09-18 **【活動內容】**

	本課程針對生成式 AI 在資安領域的應用與挑戰深入探討，涵蓋社交工程攻擊、深偽技術（Deepfake）偵測、AI 資安防禦技術、資料保護機制，以及 AI 應用中的挑戰。透過案例分析與實務應用，說明如何運用 AI 技術進行異常行為分析、威脅預測與應變處置，並探討 AI 治理、模型偏見與倫理議題，協助資安人員提升面對 AI 資安威脅的應對能力與實務操作知識。 **【主辦單位】中華民國資訊軟體服務商業同業公會** **【聯絡窗口】02-2553-3988#816 林專員** **security@tissa.org.tw**
【資安學院】10/1-惡意程式偵測、 分析與防護解析班	
活動時間	**2026-10-01 09:00 ~ 2026-10-01 16:00**
活動地點	**中華軟體公會──大同辦公室D01會議室（ 臺北市中山北路三段22-1號新社工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5918**
活動概要	**【費用】** 原價：7,200元/人 早鳥價：6,800元/人 公會會員：6,000元/人 費用含稅、教材、餐點及完課證明 報名截止：2026-09-29 **【活動內容】** 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】中華民國資訊軟體服務商業同業公會**

	【聯絡窗口】02-2553-3988#816 林專員 **security@tissa.org.tw**
【資安學院】10/13~10/14-iPAS-「初級」資訊安全工程師-能力研習衝刺班	
活動時間	**2026-10-13 09:00 ~ 2026-10-14 16:00**
活動地點	**中華軟體公會──大同辦公室D01會議室（ 臺北市中山北路三段22-1號新社工大樓5樓C區 ）**
活動網站	**https://www.tissa.org.tw/Course/Detail/5895**
活動概要	**【費用】** 原價：11,000元/人 早鳥價：9,900元/人 公會會員：8,500元/人 費用含稅、教材、餐點及完課證明 報名截止：2026-10-09 **【活動內容】** 本課程將使學員瞭解資訊安全管理與技術專有名詞及其代表意義，並具備資訊安全管理基礎知識，如：資產與風險管理、存取控制、身分認證、事故管理、營運持續、法規遵循與資訊倫理等。 **【主辦單位】中華民國資訊軟體服務商業同業公會** **【聯絡窗口】02-2553-3988#816 林專員** **security@tissa.org.tw**
【資安學院】11/6-LINUX 暨 WINDOWS 鑑識處理	
活動時間	**2026-11-06 09:00 ~ 2026-11-06 17:00**
活動地點	**國立中興大學**
活動網站	**https://www.tissa.org.tw/Course/Detail/5922**
	【費用】 原價：8,500元/人

活動概要	早鳥價：8,000元/人 公會會員：7,500元/人 費用含稅、教材、餐點及完課證明 報名截止：2026-11-03 **【活動內容】** 本課程目標在於模擬 LINUX 系統受駭的情境，解析駭客針對 LINUX 系統可能發動的攻擊，並介紹相關工具進行鑑識處理。此外，亦於課程中將 LINUX 及 WINDOWS 鑑識處理進行比較 ，說明兩者之異同及須特別注意之事項。 **【主辦單位】中華民國資訊軟體服務商業同業公會** **【聯絡窗口】02-2553-3988#816 林專員** **security@tissa.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：

二一零零科技｜公文管理系統 - Arbitrary File Upload	
TVN / CVE ID	TVN-202608001 / CVE-2026-74845
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	公文管理系統 5.0.105(不含)以前版本
問題描述	二一零零科技開發之公文管理系統存在Arbitrary File Upload漏洞，已通過身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼。
解決方法	請更新至5.0.105(含)以後版本
公開日期	2026-08-17
相關連結	**https://www.twcert.org.tw/tw/cp-132-11108-7b14c-1.html**
美麗島安全科技｜4MOSAn GCB Doctor - OS Command Injection	
TVN / CVE ID	TVN-202608004 / CVE-2026-78211
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	4MOSAn GCB Doctor 20260621(不含)以前
問題描述	美麗島安全科技開發之4MOSAn GCB Doctor存在OS Command Injection漏洞，未經身分鑑別之遠端攻擊者可透過未移除之ADOdb測試頁面參數注入惡意指令，進而於伺服器端執行任意系統指令。
解決方法	更新至20260621(含)以後版本，並執行 FreeBSD-GCB 管理中心安全升級

公開日期	2026-08-24
相關連結	**https://www.twcert.org.tw/tw/cp-132-11118-dfee4-1.html**
樂衍有限公司｜樂晴醫事管理系統 - Remote Code Execution	
TVN / CVE ID	TVN-202608007 / CVE-2026-78685
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	樂晴醫事管理系統 2.4.2.8 至 2.5.1.9 版本
問題描述	【CVE-2026-78685(Remote Code Execution)】 未經身分鑑別之遠端攻擊者可利用特製HTML網頁執行任意作業系統指令。
解決方法	更新至2.5.2.0(含)以後版本
公開日期	2026-08-25
相關連結	**https://www.twcert.org.tw/tw/cp-132-11127-cda76-1.html**
思考軟體科技｜EFence - 存在2個漏洞	
TVN / CVE ID	TVN-202608010 / CVE-2026-80235, CVE-2026-80237
CVSS	【CVE-2026-80235】 9.8(Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 【CVE-2026-80237】 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	EFence 1.2.66 DB Ver:56(含)以前版本
問題描述	【CVE-2026-80235(Arbitrary File Upload)】 未經身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼。 【CVE-2026-80237(Arbitrary File Upload)】

	已通過身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼。
解決方法	請更新至1.2.67 DB Ver:57(含)以後版本
公開日期	2026-08-26
相關連結	**https://www.twcert.org.tw/tw/cp-132-11133-e0167-1.html**
綠色運算｜NUMail - OS Command Injection	
TVN / CVE ID	TVN-202608011 / CVE-2026-82082
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	NUMail所有版本
問題描述	綠色運算開發之NUMail存在OS Command Injection漏洞，未經身分鑑別之遠端攻擊者可注入任意作業系統指令並於伺服器上執行。
解決方法	廠商已完成漏洞修補並派發更新，請確認是否已更新Patch至202602162(含)以後版本
公開日期	2026-08-28
相關連結	**https://www.twcert.org.tw/tw/cp-132-11144-45c6a-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：**2026年8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/**