TWCERT/CC 資安情資電子報

2025 年 11 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

全球網路威脅活動「Operation WrtHug」鎖定華碩 (ASUS) 路由器，呼籲用戶立即更新韌體

資安廠商SecurityScorecard的 STRIKE 團隊近日發布的一份重要報告，揭露了一項代號為 「Operation WrtHug」 的大規模網路行動。此行動正鎖定全球 華碩 (ASUS) 相關之路由器，利用已知漏洞將感染設備變成全球網路威脅活動的工具。TWCERT特此發布緊急警示，強烈建議所有華碩路由器用戶立即採取必要措施，確保資訊安全。

什麼是「Operation WrtHug」？

Operation WrtHug 是一個針對小型/家用路由器進行的持續性攻擊活

動，目前觀察主要集中ASUS品牌，攻擊者主要針對華碩設備上的AiCloud 服務，利用一系列已公開的 作業系統指令注入（OS Command Injection）漏洞（例如與 CVE-2023-39780 相關的漏洞）作為初始存取點，目前觀察到影響華碩8個產品型號。

項次	型號
▪1	ASUS Wireless Router 4G-AC55U
▪2	ASUS Wireless Router 4G-AC860U
▪3	ASUS Wireless Router DSL-AC68U
▪4	ASUS Wireless Router GT-AC5300
▪5	ASUS Wireless Router GT-AX11000
▪6	ASUS Wireless Router RT-AC1200HP
▪7	ASUS Wireless Router RT-AC1300GPLUS
▪8	ASUS Wireless Router RT-AC1300UHP

表1：被攻擊之路由器型號。資料來源： SecurityScorecard

一旦路由器被成功入侵，駭客將會植入後門程式，使設備加入一個龐大的全球感染網路，被用作發動進一步的網路威脅活動及間諜行動。STRIKE 團隊在過去六個月中，已識別出全球超過 50,000 個 IP 設備被感染。

用戶應立即採取的關鍵步驟（緩解措施）

由於攻擊者利用的都是已公開且已有修補程式的漏洞，確保設備的

安全至關重要。請所有用戶立即採取以下三項關鍵行動：

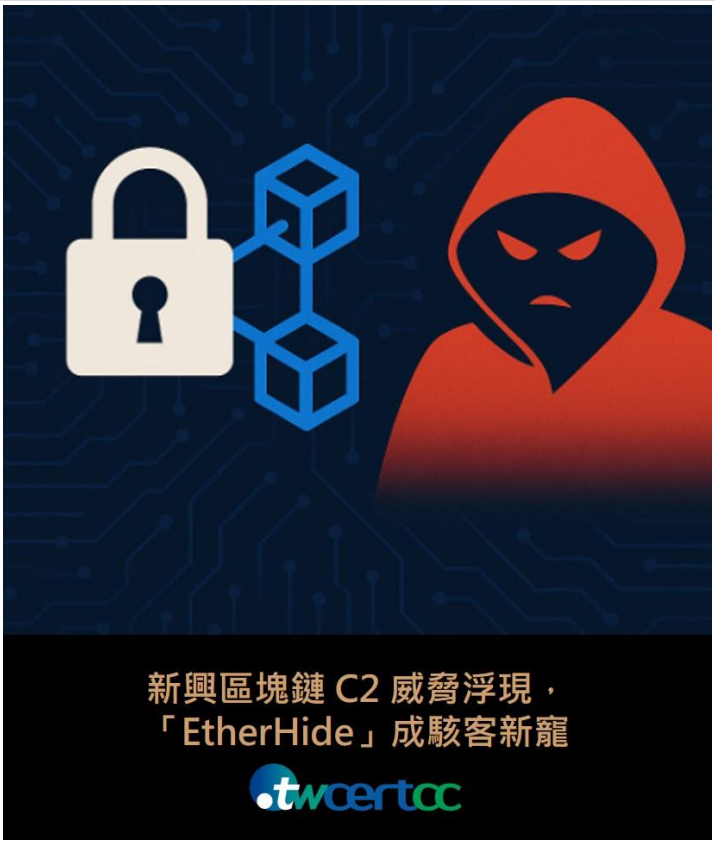
1. 執行韌體更新是關鍵： 請務必將您的路由器韌體更新到最新版本。這是修補已知漏洞、防止入侵的最直接方法。
2. 檢查並汰換 EoL 設備： 如果您使用的是已「終止支援」（End-of-Life, EoL）的舊款 ASUS 路由器，無法更新韌體，請考慮將這些老舊設備替換為官方仍持續支援的新產品。
3. 諮詢官方資源： 華碩安全團隊已針對 Operation WrtHug 中涉及的所有漏洞提供了官方緩解步驟 (https://www.asus.com/content/asus-product-security-advisory/)。請用戶務必查閱 ASUS 產品安全建議或相關 FAQ，以取得最準確的防護資訊。

- 相關連結
  1. Operation WrtHug, The Global Espionage Campaign Hiding in Your Home Router

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 新興區塊鏈 C2 威脅浮現，「EtherHide」成駭客新寵



隨著Web3與智能合約技術日益成熟，資安威脅也呈現新型演化，攻擊者開始利用區塊鏈平台做為命令與控制（Command & Control, C2）架構。2023年10月，資安研究人員首次提出一種名為「EtherHide」的技術，該技術運用區塊鏈的去中心化、不可篡改及匿名性特性，攻擊者將C2惡意指令或惡意酬載(Payload)地址寫入智能合約(Smart Contracts)中，從而繞過傳統網路防禦機制如域名攔截、IP封鎖和流量監控，提高C2架構的隱蔽性。

EtherHide技術是將惡意酬載或指令寫入區塊鏈上的智能合約，使惡意程式得以在感染階段與後續攻擊階段，透過查詢區塊鏈取得最新指令，形成難以封鎖的 C2 通道。根據多起資安事件分析，EtherHide經常與偽裝更新的「ClearFake」搭配使用，先以假更新誘導下載，再由EtherHide提供後續酬載，成為攻擊者初始滲透的重要手法。

ClearFake是一種以社交工程為核心的攻擊手法，最早於2023年第2季被發現，攻擊者會在受感染的網站中，植入惡意JavaScript程式碼（實務案例多半發生在遭入侵的WordPress網站），當使用者瀏覽到這些頁面時，網站會彈出偽裝成系統通知或軟體更新的假訊息，誘導試用者點擊。一旦使用者誤點，隱藏於其中的惡意指令便會被立刻執行。圖1為常見的假通知範例。

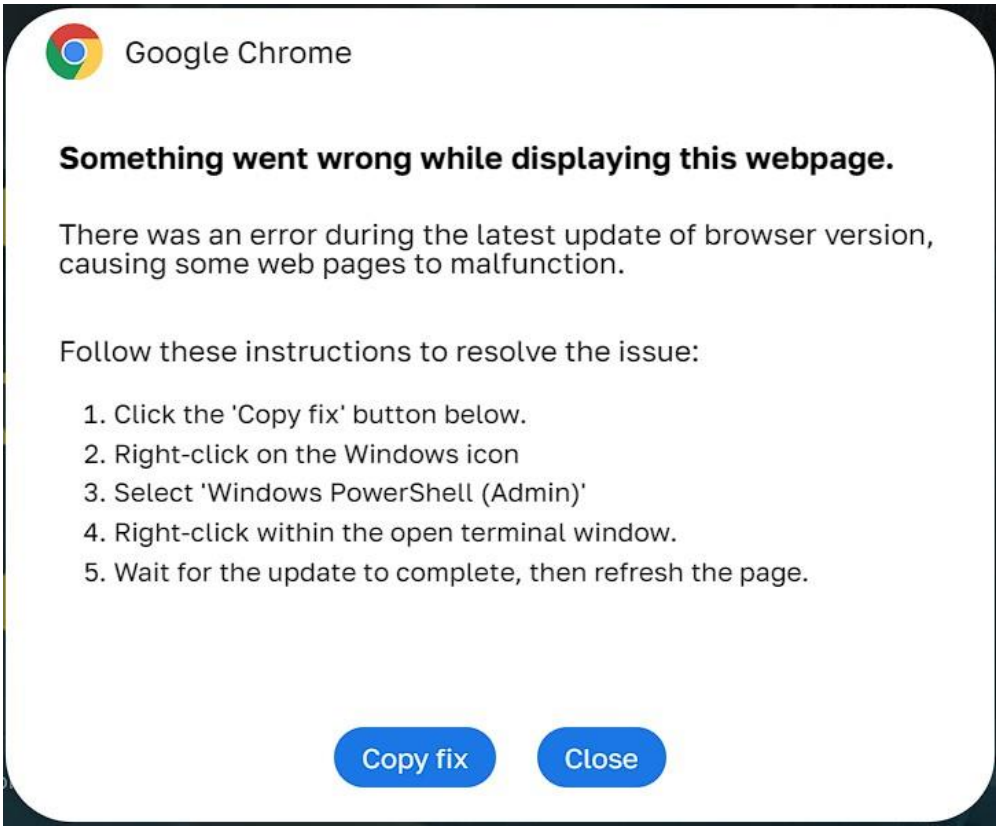


圖1：偽造系統通知或軟體更新之範例。圖片來源：wyretechnology

從2024年至今，常見的攻擊流程如下：

1. 攻擊者首先入侵存在漏洞的WordPress網站，從而取得網站的控制權
2. 取得網站控制權後，攻擊者在網站頁面植入惡意JavaScript程式碼
3. 當使用者瀏覽受感染網站時，惡意JavaScript程式碼便會被自動執行
4. 惡意程式碼彈出偽冒更新訊息(ClearFake攻擊活動)，誘騙使用者點擊
5. 當使用者點擊後，惡意JavaScript會連線至BSC(Binance Smart Chain)智能鏈上的智能合約，透過EtherHide技術取得攻擊者放於區塊鏈上的惡意指令或酬載位置
6. 根據鏈上指令，惡意JavaScript隨後下載並部署下一階段惡意程式至受害者電腦
7. 最後，惡意程式啟動並執行其既定的攻擊行為

BSC(Binance Smart Chain)是幣安在2020年推出的區塊鏈平台，支援去中心化應用和智能合約。EtherHide技術多半部署在BSC上，推測與其開發環境API的便利性有關，攻擊者普遍利用幣安SDK所提供的「eth_call」方法，此為用於讀取智能合約查詢操作，無需支付交易費用（gas），且不會在區塊鏈上留下紀錄。eth_call使惡意程式能頻繁且隱蔽與智能合約通信，無須承擔鏈上交互所需的成本與痕跡風險，因而成為攻擊者實現鏈上C2架構的利器。

EtherHide技術利用區塊鏈作為隱蔽且難以封鎖的指令來源，使攻擊

活動更具持續性與隱藏性，其吸引力包含：

1. 傳統的追蹤技術不易套用於區塊鏈環境，增加防禦的難度
2. 區塊鏈上的資料不可刪除，使惡意指令一旦部署就無法下架
3. 攻擊者無需在受害者端部署大量檔案，有效降低被偵測的風險

由於EtherHide利用區塊鏈形成難以封鎖的C2通道，且常與假更新攻擊ClearFake併用，企業需從多面向加強防護。以下為精簡防禦建議：

1. 多起真實資安事件皆源於WordPress等常見CMS的漏洞或惡意外掛，應確保核心與外掛隨時更新，並搭配Web應用防火牆（WAF）等措施，降低被植入惡意腳本的風險
2. 當受害者下載並執行惡意酬載時，仍需仰賴端點防護系統、動態行為分析與沙箱技術，來偵測惡意程式與異常活動
3. 由於攻擊鏈常透過偽裝更新或假下載頁面誘導使用者點擊，企業應定期進行社交工程演練，以提升員工對惡意更新訊息與不明通知的警覺性
4. 若敏感系統需透過節點或RPC介面與公共鏈互動，建議規劃白名單或其他存取控制機制，以避免遭惡意鏈上資料影響
5. 資安公司與防毒廠商應將EtherHide視為新型態威脅來源，並適時納入行為偵測模型與威脅情報資料庫中

- 相關連結
  1. “EtherHiding” — Hiding Web2 Malicious Code in Web3 Smart Contracts
  2. Etherhide Explained: The Rise of Blockchain-Based Command and Control
  3. EtherHiding and Fake-Updates Used to Deliver Malware
  4. WatchData Documentation-eth_call (BSC)

2.2 軟硬體系統資安議題

2.2.1 WSUS 高嚴重性漏洞 CVE-2025-59287 已遭利用，呼籲用戶儘速更新

Windows於2025年10月發布例行資安更新公告，揭露Windows Server Update Services (WSUS) 存在一個高嚴重性漏洞(CVE-2025-59287，CVSS：9.8)。該漏洞允許未經身分驗證的遠端攻擊者，透過發送精心設計的請求觸發反序列化，導致在目標伺服器上以系統權限執行任意程式碼。此漏洞僅影響啟用WSUS伺服器角色的Windows Server，預設情況下WSUS角色並未啟用。

美國網路安全與基礎設施安全局（CISA）已將CVE-2025-59287納入已知漏洞目錄(KEV)，並觀察該漏洞已被攻擊者積極利用。荷蘭國家網路安全中心（NCSC-NL）亦發布警告，確認漏洞已遭實際利用，建議用戶

儘速依循Windows官方建議，採取相關緩解措施，以防止系統遭入侵並造成重大損失。

資安業者Huntress發現攻擊者正在掃描對外開放WSUS連接埠（8530與8531），並向可連線的伺服器發送惡意請求。攻擊過程中，攻擊者可能透過PowerShell解碼並執行惡意酬載，搜尋網路內所有伺服器與使用者資訊，並將竊取的資料傳送至遠端伺服器；同時還會利用代理伺服器混淆攻擊過程。

面對此重大資安威脅，建議企業和組織採取以下防護措施：

1. 依Mirosoft安全更新指南，確認受影響版本，並將對應的安全更新(Security Patches)儘速套用至所有 WSUS 伺服器。
2. 嚴格執行服務最小化原則：除非有明確業務需求，應停用 WSUS 伺服器角色或移除不必要的WSUS部署。
3. 邊界防禦：在主機與網路邊界防火牆上，阻止/阻擋 (Block) 連接埠8530和8531的所有外部入站流量。
4. 系統安全開發：建立安全的資料序列化機制與嚴格的類型驗證，以防範不受信任的反序列化攻擊。
5. 威脅偵測：持續監控並透過日誌分析工具分析 WSUS 相關的網路流量與系統日誌，以儘早檢測任何可疑行為。

- 相關連結

1. CVE-2025-59287 WSUS Remote Code Execution
2. Exploitation of Windows Server Update Services Remote Code Execution Vulnerability (CVE-2025-59287)
3. Newly Patched Critical Microsoft WSUS Flaw Comes Under Active Exploitation
4. CISA orders feds to patch Windows Server WSUS flaw used in attacks
5. Critical WSUS flaw in Windows Server now exploited in attacks

2.3 軟硬體漏洞資訊

2.3.1 Docker Compose存在重大資安漏洞(CVE-2025-62725)

CVE 編號	CVE-2025-62725
影響產品	Docker Compose
解決辦法	更新 Docker Compose v2.40.2(含)之後版本

- 內容說明：

  Docker Compose 是用於定義與管理多個容器的應用工具，能簡化部署流程並提高開發效率。Docker 發布重大資安漏洞更新公告(CVE-2025-62725，CVSS 4.x：8.9)並釋出更新版本，此為路徑遍歷漏洞，允許攻擊者繞過 Compose 的快取目錄，進而在主機上覆寫任意檔案。

- 影響平台：
  - Docker Compose v2.40.2(不含)之前版本
- 資料來源：
  1. Path Traversal via OCI Artifact Layer Annotations
  2. CVE-2025-62725

2.3.2 Cisco旗下Unified Contact Center Express(Unified CCX)存在2個重大資安漏洞

CVE 編號	CVE-2025-20354,CVE-2025-20358
影響產品	Cisco Unified Contact Center Express
解決辦法	請更新至以下版本 Cisco Unified Contact Center Express 12.5 SU3 ES07(含)之後版本 Cisco Unified Contact Center Express 15.0 ES01(含)之後版本

- 內容說明：

  Cisco Unified Contact Center Express (Unified CCX)是一款企業建立客服中心的解決方案，整合語音、即時訊息、電子郵件等多種客服管道，提升客戶服務效率。日前，Cisco 發布重大資安漏洞公告(CVE-2025-20354，CVSS：9.8 和 CVE-2025-20358，CVSS：9.4)，CVE-2025-20354 為遠端執行程式碼漏洞，允許未經身分驗證的攻擊者在受影響的系統上傳任意檔案，使用 root 權限執行任意命令；CVE-2025-20358 為繞過身分驗證漏洞，可能允許未經身分驗證的遠端攻擊者繞過身分驗證，取得腳本建立和執行相關的管理權限。

- 影響平台：
  - Cisco Unified Contact Center Express 12.5 SU3(含)之前版本
  - Cisco Unified Contact Center Express 15.0

- 資料來源：
  1. Cisco Unified Contact Center Express Remote Code Execution Vulnerabilities
  2. CVE-2025-20354
  3. CVE-2025-20358

2.3.3 Samba存在重大資安漏洞(CVE-2025-10230)

CVE 編號	CVE-2025-10230
影響產品	Samba
解決辦法	根據官方網站釋出解決方式進行修補： https://www.samba.org/samba/history/security.html

- 內容說明：

  Samba 是一款開源軟體產品，主要用於不同作業系統間的檔案及印表機共享。近日發布重大資安漏洞公告(CVE-2025-10230，CVSS：10.0)，此漏洞為作業系統指令注入漏洞，若使用者架設 Samba AD Domain Controller 伺服器並啟用 WINS 協定支援，未經身分驗證的遠端攻擊者可注入任意作業系統指令於 Samba 伺服器上執行。

- 影響平台：
  - Samba 4.21.9(不含)以前版本
  - Samba 4.22.0 至 4.22.5(不含)版本
  - Samba 4.23.0 至 4.23.2(不含)版本
- 資料來源：
  1. Samba Security Releases
  2. CVE-2025-10230
  3. CVE-2025-10230

2.3.4 SAP針對旗下2款產品發布重大資安公告

CVE 編號	CVE-2025-42887,CVE-2025-42890
影響產品	SAP Solution Manager、SQL Anywhere Monitor
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/november-2025.html

- 內容說明：

  【CVE-2025-42887，CVSS：9.9】

  此漏洞缺少輸入清理機制，允許經過身分驗證的攻擊者呼叫遠端功能模組時，植入惡意程式碼，影響系統的機密性、完整性和可用性。

  【CVE-2025-42890，CVSS：10.0】

  SQL Anywhere Monitor (Non-GUI) 存在金鑰和金鑰管理安全漏洞，該漏洞源於程式中直接嵌入憑證，可能使未經授權的攻擊者取得系統資源或執行任意程式碼，影響系統的機密性、完整性和可用性。

- 影響平台：
  - SAP Solution Manager ST 720 版本
  - SQL Anywhere Monitor (Non-Gui) SYBASE SQL ANYWHERE SERVER 17.0 版本
- 資料來源：
  1. SAP Security Patch Day - November 2025
  2. CVE-2025-42887
  3. CVE-2025-42890

2.3.5 Microsoft SQL Server 存在重大資安漏洞(CVE-2025-59499)

CVE 編號	CVE-2025-59499
影響產品	Microsoft SQL Server
解決辦法	根據官方網站釋出解決方式進行修補： https://msrc.microsoft.com/update-guide/zh-tw/vulnerability/CVE-2025-59499

- 內容說明：

  微軟針對旗下產品 SQL Server 發布重大資安漏洞公告(CVE-2025-59499，CVSS：8.8)，此漏洞為 SQL 注入漏洞，允許經授權的攻擊者透過網路注入精心設計的 SQL 指令並提升權限。

- 影響平台：
  - Microsoft SQL Server 2017 (GDR) 14.0.0 至 14.0.2095.1 版本
  - Microsoft SQL Server 2019 (GDR) 15.0.0 至 15.0.2155.2 版本
  - Microsoft SQL Server 2016 Service Pack 3 (GDR) 13.0.0 至 13.0.6475.1 版本
  - Microsoft SQL Server 2016 Service Pack 3 Azure Connect Feature Pack 13.0.0 至 13.0.7070.1 版本
  - Microsoft SQL Server 2017 (CU 31) 14.0.0 至 14.0.3515.1 版本
  - Microsoft SQL Server 2022 (GDR) 16.0.0 至 16.0.1160.1 版本
  - Microsoft SQL Server 2019 (CU 32) 15.0.0.0 至 15.0.4455.2 版本
  - Microsoft SQL Server 2022 (CU 21) 16.0.0.0 至 16.0.4222.2 版本
- 資料來源：
  1. Microsoft SQL Server Elevation of Privilege Vulnerability
  2. CVE-2025-59499

2.3.6 Cisco旗下Catalyst Center存在重大資安漏洞(CVE-2025-20341)

CVE 編號	CVE-2025-20341
影響產品	Cisco Catalyst Center
解決辦法	請更新至以下版本： Cisco Catalyst Center 2.3.7.10-VA(含)之後版本

- 內容說明：

  Catalyst Center是Cisco提供的網路管理平台，藉由自動化配置和部署功能，可協助網路管理人員更有效率管理和監控企業網路環境。近日，Cisco 發布重大資安漏洞公告(CVE-2025-20341，CVSS：8.8)，該漏洞源於使用者輸入資料驗證不足，允許攻擊者可向受影響的系統發送精心設計的 HTTP 請求，對系統進行未授權的修改。

  備註：攻擊者若要使用此漏洞，必須至少具有「Observer」角色的有效憑證

- 影響平台：
  - Cisco Catalyst Center 2.3.7.3-VA 至 2.3.7.10-VA(不含)之前版本
- 資料來源：
  1. Cisco Catalyst Center Virtual Appliance Privilege Escalation Vulnerability
  2. CVE-2025-20341

2.3.7 Fortinet旗下FortiWeb存在重大資安漏洞(CVE-2025-64446)

CVE 編號	CVE-2025-64446
影響產品	FortiWeb
解決辦法	請更新至以下版本： FortiWeb 7.0.12 版本 FortiWeb 7.2.12 版本 FortiWeb 7.4.10 版本 FortiWeb 7.6.5 版本 FortiWeb 8.0.2 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-2025-64446，CVSS：9.8)，此漏洞為相對路徑遍歷漏洞，可能允許未經身分驗證的攻擊者，透過精心設計的 HTTP 或 HTTPs 請求，在系統上執行管理命令。

  備註：目前 Fortinet 已觀察到有攻擊者利用此漏洞，建議儘速採取暫時緩解措施，以防止針對此漏洞可能的攻擊發生。

- 影響平台：
  - FortiWeb 7.0.0 至 7.0.11 版本
  - FortiWeb 7.2.0 至 7.2.11 版本
  - FortiWeb 7.4.0 至 7.4.9 版本
  - FortiWeb 7.6.0 至 7.6.4 版本
  - FortiWeb 8.0.0 至 8.0.1 版本
- 資料來源：
  1. Path confusion vulnerability in GUI
  2. CVE-2025-64446

2.3.8 Fortinet旗下FortiVoice存在SQL注入漏洞(CVE-2025-58692)

CVE 編號	CVE-2025-58692
影響產品	FortiVoice
解決辦法	請更新至以下版本： FortiVoice 7.0.8 版本 FortiVoice 7.2.3 版本

- 內容說明：

  FortiVoice 是 Fortinet 是一款提供企業的通訊系統，整合語音通話、會議、聊天和傳真等功能，支援混合和遠端工作環境。近日，Fortinet 發布重大資安漏洞公告(CVE-2025-58692，CVSS：8.8)，此漏洞為 SQL 注入漏洞，允許經過身分驗證的攻擊者，透過精心設計的 HTTP 或 HTTPs 請求，執行未經授權的程式碼或指令。

- 影響平台：
  - FortiVoice 7.0.0 至 7.0.7 版本
  - FortiVoice 7.2.0 至 7.2.2 版本
- 資料來源：
  1. SQL injections in voice and administrative interface
  2. CVE-2025-58692

2.3.9 SolarWinds旗下Serv-U軟體存在3個重大資安漏洞

CVE 編號	CVE-2025-40547,CVE-2025-40548,CVE-2025-40549
影響產品	SolarWinds Serv-U
解決辦法	請更新至以下版本： SolarWinds Serv-U 15.5.3 版本

- 內容說明：

  SolarWinds Serv-U 是一款用於安全文件傳輸的伺服器軟體，支援 FTP、FTPS、SFTP 等多種協議，具備易用的管理介面，並支援跨平台與跨裝置存取等功能。日前，SolarWinds 發布旗下產品 Serv-U 存在 3 個重大資安漏洞。

  【CVE-2025-40547，CVSS：9.1】

  此為邏輯錯誤漏洞，可能允許具有管理員權限的攻擊者可執行程式碼。

  【CVE-2025-40548，CVSS：9.1】

  此為缺失驗證過程漏洞，可能允許具有管理員的攻擊者可執行程式碼。

  【CVE-2025-40549，CVSS：9.1】

  此為路徑限制繞過漏洞，可能允許具有管理者權限的攻擊者，可在目錄上執行程式碼。

- 影響平台：
  - SolarWinds Serv-U 15.5.2.2.102 版本

- 資料來源：
  1. SolarWinds Serv-U Logic Abuse - Remote Code Execution Vulnerability (CVE-2025-40547)
  2. SolarWinds Serv-U Broken Access Control - Remote Code Execution Vulnerability (CVE-2025-40548)
  3. SolarWinds Serv-U Path Restriction Bypass Vulnerability (CVE-2025-40549)
  4. CVE-2025-40547
  5. CVE-2025-40548
  6. CVE-2025-40549

第 3 章、資安研討會及活動

- **資安研討會**

2025 台灣資安通報應變年會：打造安全產品 串聯信任防線	
活動時間	**2025年12月03日 星期三**
活動地點	**臺大醫院國際會議中心 301廳(台北市中正區徐州路2號3樓)**
活動網站	**https://activity.twcert.org.tw/2025/index.htm**
活動概要	**【費用】** 免費 **【活動形式】** 實體與線上混合型會議(會場座席有限，開放TWCERT/CC會員優先參與且額滿為止) **【參加對象】** 國內各大企業、中小企業經營者、製造業者、高科技產業、資安領域相關業者、CERT/CSIRT組織、ISAC組織、SOC組織與對資安主題有興趣之單位。 **【活動內容 / Event Deails】** TWCERT/CC 主辦之台灣資安通報應變年會邁入第九屆，本次年會以「打造安全產品 串聯信任防線」為主題，聚焦資安趨勢與通報應變，從 AI 驅動下的新興威脅、台灣通報協調機制的成果與挑戰，到如何將通報落實為有效應變；進一步探討產品資安實務，從 Secure-by-Design 設計理念、PSIRT 弱點通報到供應鏈協作，剖析產品安全與品牌信任間的緊密關聯。期盼透過經驗交流與趨勢分享，強化企業與組織對資安通報、聯防協作及產品資安治理的實戰能力，打造更具韌性的資安生態。

	【指導單位】數位發展部 【主辦單位】數位發展部資通安全署、台灣電腦網路危機處理暨協調中心（TWCERT/CC） 【承辦單位】國家資通安全研究院 【報名洽詢】02-8729-1099#211 吳小姐 Evelyn.Wu@taiwan.messefrankfurt.com
【中華軟協】零信任思維下的 Mac 生態：從合規到主動防禦（北中南三場）	
活動時間	北部場：11月 27日(四) 13：30-16：30 南部場：12月 2日(二) 13：30-16：30 中部場：12月 3日(三) 13：30-16：30
活動地點	北部場：集思北科大會議中心2F＋3F 感恩廳 南部場：資安暨智慧科技研發大樓 A121國際會議廳 中部場：臻愛花園飯店台中烏日館 第一廳
活動網站	https://www.cisanet.org.tw/News/Detail/7216
活動概要	 【費用】 免費 【活動內容 / Event Deails】

	根據國際資安威脅報告指出，2024 年全球針對政府與公共部門的攻擊事件較前一年成長近 40%，臺灣更是平均每日更遭受超過 240 萬次惡意連線。隨著資通安全法正式三讀通過，政府部門資安治理邁入了新階段！ 面對資安威脅常態化的挑戰，公部門及企業皆以「零信任架構」與「合規治理」為核心，推動全面資安強韌化。從制度到技術，如何確保每一台終端設備都能符合防護標準，成為各單位稽核與查核的重點。 本場次將聚焦在公部門環境的安全挑戰與治理策略，探討如何透過身份驗證、設備信任與政策落實，打造可稽核、可管理、可持續的防禦機制。邀請您一同參與，了解如何從合規出發，邁向主動防禦的零信任新時代，為政府資安治理開啟新篇章！ **【主辦單位】中華民國資訊軟體協會** **【執行單位】中華龍網股份有限公司、捷飛科技股份有限公司、可立可股份有限公司、一休資訊股份有限公司、中華電信股份有限公司** **【聯絡窗口】02-2553-3988#388 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：

一等一科技｜U-Office Force - 存在2個漏洞	
TVN / CVE ID	TVN-202511002 / CVE-2025-12864, CVE-2025-12865
CVSS	CVE-2025-12864： 8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CVE-2025-12865： 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	U-Office Force 29.50(不含)以前版本
問題描述	CVE-2025-12864(SQL Injection)： 已驗證之遠端攻擊者可注入任意SQL指令讀取、修改及刪除資料庫內容。 CVE-2025-12865(SQL Injection)： 已驗證之遠端攻擊者可注入任意SQL指令讀取、修改及刪除資料庫內容。
解決方法	更新至29.50(含)以後版本
公開日期	2025-11-10
相關連結	**https://www.twcert.org.tw/tw/cp-132-10488-2df22-1.html**
百加資通｜EIP Plus - Weak Password Recovery Mechanism	
TVN / CVE ID	TVN-202511003 / CVE-2025-12866
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	EIP Plus RELEASE_240626(不含)以前版本
問題描述	CVE-2025-12866(Weak Password Recovery Mechanism)：

	未經身分鑑別之遠端攻擊者可預測或暴力破解忘記密碼連結，進而成功修改任意使用者密碼。
解決方法	更新至RELEASE_240626(含)以後版本
公開日期	2025-11-10
相關連結	https://www.twcert.org.tw/tw/cp-132-10490-2534b-1.html
網韻資訊｜New Site Server - Use of Client-Side Authentication	
TVN / CVE ID	TVN-202511004 / CVE-2025-12868
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	New Site Server
問題描述	網韻資訊開發之New Site Server存在Use of Client-Side Authentication漏洞，未經身分鑑別之遠端攻擊者可修改前端程式碼取得網站管理者權限。
解決方法	聯繫廠商進行更新
公開日期	2025-11-10
相關連結	https://www.twcert.org.tw/tw/cp-132-10493-bf807-1.html
育碁數位科技｜eHRD - 存在2個漏洞	
TVN / CVE ID	TVN-202511005 / CVE-2025-12870, CVE-2025-12871
CVSS	CVE-2025-12870： 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVE-2025-12871： 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)以前版本
問題描述	CVE-2025-12870：

	a+HRD存在Authentication Abuse漏洞，未經身分鑑別之遠端攻擊者可發送特定封包取得管理權限憑證，使用該憑證可以管理員權限存取系統。 CVE-2025-12871： a+HRD存在Authentication Abuse漏洞，未經身分鑑別之遠端攻擊者可自行製作管理權限憑證，並使用該憑證以管理員權限存取系統。
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	2025-11-12
相關連結	https://www.twcert.org.tw/tw/cp-132-10486-a3459-1.html
元岡科技｜ThinPLUS - OS Command Injection	
TVN / CVE ID	TVN-202511010 / CVE-2025-13284
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	ThinPLUS TPmCloud4.0
問題描述	元岡科技開發之ThinPLUS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	請更新至 TPmCloud4.2(含)以後版本
公開日期	2025-11-17
相關連結	https://www.twcert.org.tw/tw/cp-132-10512-e196b-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11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/**