



TWCERT/CC 資安情資電子報

TWCERT/CC 資安情資電子報

2026 年 9 月份

2026 年 9 月 1 日

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

目錄 II

第 1 章、封面故事.....	1
Microsoft發布Exchange Server系列安全性更新，CVE-2026-62911已有攻擊利用程式碼流通，籲儘速修補.....	1
第 2 章、國內外重要資安事件.....	4
2.1 國際政府組織資安資訊.....	4
2.1.1 CISA更新Medusa勒索軟體安全防護指引：揭露新型勒索手法與入侵指標.....	4
2.2 軟硬體系統資安議題.....	8
2.2.1 PostgreSQL潛藏12年高風險漏洞，恐導致任意程式碼執行.....	8
2.3 軟硬體漏洞資訊.....	11
2.3.1 SonicWall 旗下SMA1000系列產品存在重大資安漏洞 (CVE-2026-83548)	11
2.3.2 MongoDB BI Connector ODBC Driver存在高風險安全漏洞(CVE-2026-19001)，請儘速確認並進行修補.....	12
2.3.3 Splunk Enterprise存在多項高風險安全漏洞，請儘速確認並進行修補.....	13
2.3.4 Zimbra Collaboration存在高風險安全漏洞(CVE-2026-73570)，請儘速確認並進行修補.....	15
2.3.5 SonicWall NSM On-Prem 存在2個重大資安漏洞	16
2.3.6 Cisco 旗下 Nexus 9000系列交換器存在重大資安漏洞(CVE-2026-20212).....	17
2.3.7 Cisco IOS XR Software 存在5個重大資安漏洞.....	18
2.3.8 WatchGuard 旗下 Fireware OS ikes 存在3個重大資安漏洞.....	19

2.3.9	Ivanti Neurons for ITSM存在8個高風險資安漏洞	21
2.3.10	Ivanti旗下Endpoint Manager Mobile (EPMM)存在重大資安漏洞(CVE-2026-18851)	23
2.3.11	Fortinet旗下FortiSandbox、FortiSandbox Cloud 和 FortiSandbox PaaS存在重大資安漏洞 (CVE-2026-26084)	24
2.3.12	Fortinet Privileged Access Agent Chrome Extension存在重大資安漏洞(CVE-2026-84388) .	25
2.3.13	FortiMonitorOnSight存在重大資安漏洞(CVE-2026-84390)	26
2.3.14	MikroTik RouterOS 存在3個重大資安漏洞.....	27
2.3.15	Cisco Secure Email Gateway 存在重大資安漏洞(CVE-2026-76461).....	29
2.3.16	SAP針對旗下多款產品發布重大資安公告	30
2.3.17	Check Point 旗下產品Security Gateway、Security Management Server與Spark Firewall存在2個重大資安漏洞.....	32
2.3.18	Cisco Secure Email Gateway 和 Secure Email and Web Manager存在4個重大資安漏洞	34
2.3.19	Microsoft針對旗下多款產品發布重大資安公告	36
第 3 章、資安研討會及活動		37
第 4 章、TVN 漏洞公告		42
編輯：TWCERT/CC 團隊.....		46

第 1 章、封面故事

Microsoft發布Exchange Server系列安全性更新，CVE-2026-62911已有攻擊利用程式碼流通，籲儘速修補



微軟於2026年8月11日發布Exchange Server安全性更新，共修補7項CVE漏洞。其中，CVE-2026-62911已有攻擊程式，荷蘭國家網路安全中心（NCSC-NL）亦發布相關示警，另依Shadowserver Foundation監測資料，目前仍可觀察部分Exchange Server受到該漏洞影響，使用相關產

品之單位應確認版本及更新狀態，並完成安全性更新。

微軟公告

微軟於2026年8月11日發布Exchange Server安全性更新，適用於Exchange Server 2016、2019及訂閱版（SE），共修補以下7項CVE漏洞：

CVE編號	漏洞類型	CVSS基礎分數
CVE-2026-62910	權限提升	7.2
CVE-2026-62911	權限提升	8.0
CVE-2026-62912	阻斷服務	6.5
CVE-2026-62913	遠端程式碼執行	8.8
CVE-2026-65813	權限提升	6.5
CVE-2026-62914	偽造／偽冒	7.3
CVE-2026-62915	安全功能繞過	6.5

表1：微軟於2026年8月11日發布Exchange Server安全性更新（資料來源：Microsoft Exchange Server 訂閱版本 RTM 的安全性更新說明）

荷蘭國家網路安全中心（The National Cyber Security Centre ,NCSC-NL）於2026年8月28日發布警告，將CVE-2026-62911列為嚴重等級，指出已有攻擊利用程式碼（exploit code）於網路上出現。受影響版本為Exchange Server 2016、2019及訂閱版，NCSC-NL建議使用相關版本的單位應儘速安裝安全性更新，若無法立即更新，應限制Exchange Server僅供內部網路存取。

此外，Shadowserver Foundation於2026年9月1日表示，已針對CVE-2026-62911進行每日掃描及持續監測。截至2026年8月31日，全球仍有至少21,899個IP位址可觀察到未完成修補狀態，其中美國約6,200個、德國約5,100個。而台灣的部分，8月27日至9月1日期間約有250至280台Exchange伺服器暴露於網際網路且尚未修補，自9月1日起，此數量明顯

攀升，至9月4日達到約630台。

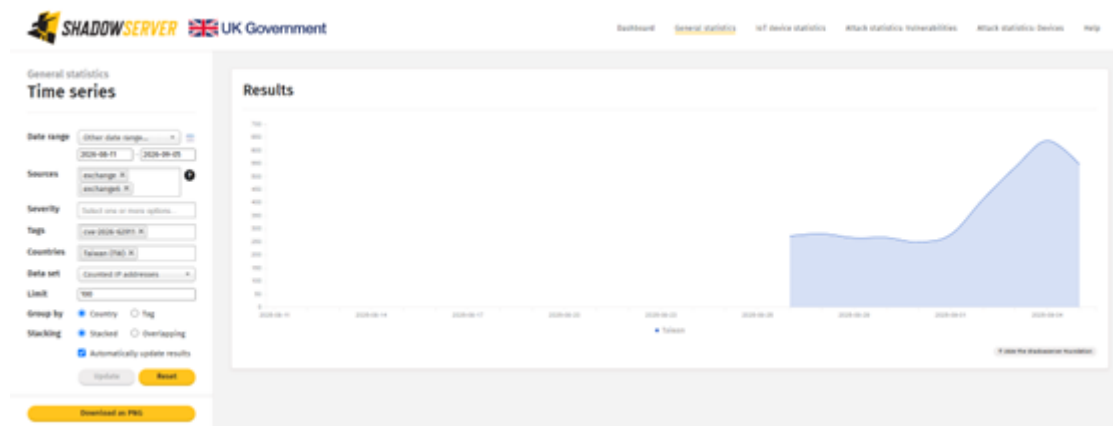


圖1：台灣暴露於網際網路且尚未完成修補之Exchange伺服器數量
(資料來源：Shadowserver General Statistics Time Series，統計區間：
8/11-9/7)

建議措施：

1. 儘速安裝微軟已發布之Exchange Server安全性更新，確認相關伺服器均已完成修補。
2. 若無法立即完成更新，應將Exchange Server伺服器限制僅供內部網路存取，降低遭受外部攻擊的風險；另針對Exchange Server 2016及2019評估版本汰換，升級至目前仍受支援之版本。

● 相關連結

1. [Microsoft Exchange Server 訂閱版本 RTM 的安全性更新說明：2026年8月11日 \(KB5121573\)](#)
2. [Ernstige kwetsbaarheden in Microsoft Exchange Server \(NCSC-NL 警示 \)](#)
3. [Shadowserver Foundation - Bluesky 貼文 \(2026/9/1，CVE-2026-62911掃描統計 \)](#)

第 2 章、國內外重要資安事件

2.1 國際政府組織資安資訊

2.1.1 CISA更新Medusa勒索軟體安全防護指引：揭露新型勒索手法與入侵指標



美國聯邦調查局（FBI）、網路安全和基礎設施安全局（CISA）及衛生及公共服務部(HHS)近日聯合發布針對勒索軟體「Medusa」的安全防護指引更新。報告指出，截至2026年4月，該勒索軟體在全球已造成超過500家機構受害，受影響範圍涵蓋醫療、教育、製造及科技等多個關鍵基礎設施領域。

Medusa自2021年6月首度被發現，近年演變為採用「勒索軟體即服務」(RaaS)的加盟營運模式，其主要入侵手法與技術特徵如下：

1. 結合初期存取仲介（IAB）：攻擊者常於網路犯罪論壇向初期存

取仲介購買受害機構的內網存取權限。

2. 快速利用已知資安漏洞：攻擊者密切關注新發布的漏洞訊息，最快能在漏洞公開後的24小時內迅速發動攻擊，鎖定尚未完成安全性修補的系統。

3. 雙重勒索機制：除將受害者裝置內的檔案加密外，還會威脅若不支付贖金，便會將竊取的資料公布在特設的洩密網站上。

此次更新中特別揭露一起重複索賠案例：受害者在支付贖金後，隨即遭到另一名自稱Medusa成員的人士聯繫，聲稱先前的談判代表已私吞款項，要求受害者必須再次支付原金額的一半，才能取得真正的解密金鑰。

此案例顯示這類惡意活動可能存在「三重勒索」新型態手段，或反映出該組織內部管理混亂且缺乏誠信。對此，FBI與CISA強烈建議所有受害機構與個人切勿支付任何贖金，因為付款不保證能復原檔案，反而可能助長惡意勒索活動。

TWCERT/CC觀察近期勒索軟體攻擊活動樣態，攻擊者可能先入侵企業內容，竊取帳號與資料，再進一步探索企業內部網路架構、取得更多系統權限並進行橫向移動，最終對大量設備進行加密，造成企業營運中斷。面對此類威脅，企業除應強化帳號與權限管理、落實多因素驗證及系統漏洞修補，也應加強內部網路分段、端點偵測與異常行為監控，並建立獨立且可還原的備份機制，以降低遭受大規模勒索攻擊時的衝擊。

雖然該勒索軟體主要以大型機構或企業為目標，但其常用的入侵技術（如釣魚信件與軟體漏洞利用）同樣影響一般個人的數位安全。為防範此類勒索軟體威脅，各組織應落實以下防護措施：

1. 啟用多因素驗證（MFA）：針對所有系統服務（特別是 Webmail、

- VPN 及關鍵系統帳戶) 強制啟用多因素驗證 (MFA) 。
2. 強化弱點管理與修補：即時更新作業系統、應用程式及韌體，並依據CISA之「已知遭利用漏洞 (KEV) 」清單優先執行安全性修補。
 3. 實施網路分段：進行內部網路區域劃分與存取控制，以遏止勒索軟體在系統間橫向移動。
 4. 監管遠端管理與控制軟體：定期稽核合法的遠端工具 (如 ConnectWise 、 BeyondTrust 、 RDP) ，停用非必要或未授權的遠端存取連線，阻擋非信任來源的內部遠端服務。
 5. 限制指令碼與命令列工具權限：限制一般使用者與低權限帳戶執行 PowerShell 或 Windows 命令提示字元 (cmd.exe) 等管理工具，降低攻擊者提升權限與偵察的能力。
 6. 落實離線備份：定期執行關鍵資料備份，確保備份資料存放於與主網路物理隔離之離線安全環境。
 7. 加強密碼安全原則：遵循國際標準，採用長度足夠的強密碼，並避免過度頻繁的強制變更密碼要求，以免衍生弱密碼風險。
 8. 部署端點偵測與回應 (EDR) 及流量稽核：導入端點偵測與回應 (EDR) 方案並搭配網路監控，即時識別並阻斷異常的橫向連線。

為協助企業與組織識別並防範此類資安威脅，以下彙整FBI於調查期間收集之Medusa勒索軟體相關最新入侵指標 (IoC) ：

類型	IoC
IP	143.244.47[.]89
IP	167.88.166[.]173
URL	https://3324.requestcatcher[.]com/hihi
IP & URL	143.110.243[.]154 (或 erp.ranasons[.]com)
IP	185.238.231[.]16
IP	23.234.89[.]195

IP	146.70.172[.]247
IP	155.2.215[.]71
IP	23.234.106[.]242
IP	23.234.93[.]112
IP	37.19.21[.]180
IP	155.2.215[.]69
IP	185.238.231[.]98
IP	37.221.66[.]239
IP	185.135.86[.]185
IP	83.138.53[.]139
IP	185.238.231[.]4
IP	185.238.231[.]77
IP	185.238.231[.]85
IP	85.155.186[.]121
URL	http://45.61.150[.]94:8000/storm[.]exe
IP	94.156.67[.]145

檔名	Hash
j.exe	2C7F328FEEB94608AAAF99EC70CB0323
def.exe	D796259C44BE852327623FD2E40C47F2
nezha-agent.exe	4D0B6E3C9C33550A005E41663A1977CB
mimilib.dll	eb05429d25fc57b476428cdb0a134b2f
command.cmd	04b13b6cd5e5291b1cde78975a140feea 7fd3bc3777c53caa1ab33426c83bfcc
RunFileCopy.cmd	b29defbbc4ebaa243c1712ccc4943374f 1b6fb864c39ed9f70fceb17eee098db
openrdp.bat	44370f5c977e415981feb7dbb87a85c
Ngconf.txt	8f11d9067da087cb4185fa804caac2df
Main_new.exe	2df705c9be0465f1c73a9f5d35147723deb16b5e

● 相關連結

1. [#StopRansomware:Medusa Ransomware](#)

2.2 軟硬體系統資安議題

2.2.1 PostgreSQL潛藏12年高風險漏洞，恐導致任意程式碼執行



Cyera Research於2026年9月1日公開研究報告，揭露PostgreSQL邏輯解碼（Logical Decoding）功能存在一項漏洞，編號為CVE-2026-6471，CVSS分數為7.2，並命名為「PostGRESshell」。具REPLICATION權限的非超級使用者（non-superuser）可利用此漏洞執行任意程式碼。PostgreSQL Global Development Group已於2026年8月13日釋出修補版本。截至2026年9月9日，公開資料未載明已有實際攻擊事件。

漏洞源自邏輯解碼外掛載入機制

邏輯解碼是PostgreSQL將預寫式日誌 (Write-Ahead Log, WAL) 中的資料變更轉換為外部系統可讀格式的機制，常用於資料複寫與變更資料擷取。PostgreSQL 自 2014 年發布的 9.4 版本起正式支援此功能，意味該漏洞在被發現前可能已存在12年。

此漏洞源於PostgreSQL邏輯解碼功能缺乏適當的授權檢查。已取得 REPLICATION權限的攻擊者，可透過指定邏輯解碼輸出外掛，利用該漏洞載入任意共享程式庫，進而取得 PostgreSQL服務所使用的作業系統帳號權限執行任意程式碼。

根據Cyera Research的研究報告，在Windows環境中，若PostgreSQL伺服器可對外連線至伺服器訊息區塊 (Server Message Block, SMB) 服務，攻擊者即可誘使系統從遠端網路路徑載入DLL。而在啟用NFS自動掛載的Linux或macOS環境，也能以類似方式載入遠端程式庫；至於一般Linux、Docker或Kubernetes環境，則須先具備將檔案寫入主機其他路徑的權限。惡意程式成功執行後，將取得與PostgreSQL程序相同的作業系統權限。這代表一旦REPLICATION帳號遭竊，其影響將從資料複寫權限，進一步擴大至資料庫主機層級。

官方已限制可載入的輸出外掛

PostgreSQL官方公告指出，現行受支援且受此漏洞影響的版本為14至18，應分別更新至14.24、15.19、16.15、17.11或18.6；Cyera Research補充表示，該問題最早可追溯至9.4版本，使用已停止支援(EOL)舊版本的單位應儘速升級。PostgreSQL於本次修補版本中新增output_plugin_libraries參數以限制可載入的輸出外掛(預設只允許pgoutput與test_decoding)。若使用wal2json等第三方外掛，管理者須手動納入允許清單方可正常運作。此外，Ubuntu亦於2026年8月20日發布USN-8653-1安全更新，提供相應的系統修補。

TWCERT/CC 建議企業與組織採取以下防護措施：

1. 立即更新 PostgreSQL 版本：盤點所有PostgreSQL資料庫主機，確認版本是否低於18.6、17.11、16.15、15.19或14.24；請依官方公告或作業系統套件來源儘速完成更新，若使用已停止支援(EOL)的舊版本應立即規劃升級。
2. 清查具複寫權限的帳號：全面盤點具有REPLICATION權限的角色，移除無業務需求的過高權限，並檢視相關帳號是否存在憑證共用或長期未更換等風險。
3. 嚴格限制邏輯解碼輸出外掛：版本更新後應檢查output_plugin_libraries設定，僅允許實際使用且經確認可信的輸出外掛，切勿為了相容性便利而任意放寬允許範圍。
4. 限制資料庫伺服器對外連線：防火牆應限制資料庫主機不必要的對外連線，重點封鎖SMB(Port 445)與NFS(Port 2049)流量，並停用未使用的自動掛載服務。
5. 落實異常複寫活動監控：持續監控非預期來源建立複寫槽、載入異常輸出外掛名稱及REPLICATION帳號的登入行為，並同步審查pg_hba.conf是否存在過度寬鬆的複寫存取規則。

● 相關連結

1. [CVE-2026-6471: PostgreSQL logical decoding can dlopen arbitrary file](#)
2. [PostgreSQL 18.6 Release Notes](#)
3. [PostgreSQL 9.4 Release Note](#)
4. [PostGRESHell: The database powering much of the internet had an open door for 12 years](#)
5. [USN-8653-1: PostgreSQL vulnerabilities](#)

2.3 軟硬體漏洞資訊

2.3.1 SonicWall 旗下SMA1000系列產品存在重大資安漏洞 (CVE-2026-83548)

CVE 編號	CVE-2026-83548
影響產品	SonicWall SMA1000
解決辦法	請更新至以下版本： SMA1000 Models - 6210, 7210, 8200v 產品 12.4.3-03526(含) 之後版本、 SMA1000 Models - 6210, 7210, 8200v 產品 12.5.0-02952(含) 之後版本

- 內容說明：

SonicWall 針對 SMA1000 系列產品發布重大資安漏洞(CVE-2026-83548，CVSS：10.0)，此為 SSRF 漏洞並存在於 SMA1000 系列產品設備工作介面中，未經身分驗證的遠端攻擊者可能利用此漏洞非法存取敏感功能並執行未經授權的操作。

備註：目前 SonicWall PSIRT 已調查一起案例，顯示該漏洞正被利用，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：

- SMA1000 Models - 6210, 7210, 8200v 產品 12.4.3-03453(含)以前版本
- SMA1000 Models - 6210, 7210, 8200v 產品 12.5.0-02835(含)以前版本

- 資料來源：

1. [SonicWall SMA1000 Series Appliances Affected By Multiple Vulnerabilities](#)
2. [CVE-2026-83548](#)

2.3.2 MongoDB BI Connector ODBC Driver存在高風險安全漏洞(CVE-2026-19001)，請儘速確認並進行修補

CVE 編號	CVE-2026-19001
影響產品	MongoDB BI Connector ODBC Driver
解決辦法	官方已針對漏洞釋出修補程式，請升級 MongoDB BI Connector ODBC Driver 至 1.4.9(含)以後版本。 詳細說明請參考官方公告，網址如下： https://github.com/mongodb/mongo-bi-connector-odbc-driver/releases/tag/v1.4.9

- 內容說明：
研究人員發現 MongoDB BI Connector ODBC Driver 存在整數溢位 (Integer Overflow)漏洞(CVE-2026-19001)，未經身分鑑別之遠端攻擊者可藉由傳入過長之名稱參數，造成緩衝區溢位，進而造成記憶體毀損與程式異常終止，並可能執行任意程式碼，請儘速確認並進行修補。
- 影響平台：
 - MongoDB BI Connector ODBC Driver 1.0.0 至 1.4.9(不含)版本
- 資料來源：
 1. [CVE-2026-19001](#)
 2. [mongodb](#)

2.3.3 Splunk Enterprise存在多項高風險安全漏洞，請儘速確認並進行修補

CVE 編號	CVE-2026-76253,CVE-2026-76310~76317,CVE-2026-76319,CVE-2026-76335,CVE-2026-76350~76352
影響產品	Splunk Enterprise
解決辦法	官方已針對漏洞釋出修補程式，請升級 Splunk Enterprise 至 9.4.14、10.0.9、10.2.6 或 10.4.2(含)以後版本。 詳細說明請參考官方公告，網址如下： https://advisory.splunk.com/advisories/SVD-2026-0801

- 內容說明：
研究人員發現 Splunk Enterprise 存在多項高風險安全漏洞(CVE-2026-76253、CVE-2026-76310 至 CVE-2026-76317、CVE-2026-76319、CVE-2026-76335 及 CVE-2026-76350 至 CVE-2026-76352)，其中最嚴重之 CVE-2026-76310 為不當存取控制(Improper Access Control)漏洞，未經身分鑑別之遠端攻擊者若持有嵌入式報表令牌(Token)，可下載相關搜尋工作的派送封存檔，並從中取得工作階段相關資訊，進而存取報表擁有者可存取之資料，並影響系統完整性。若報表擁有者具 admin 角色時，攻擊者甚至可執行管理作業，請儘速確認並進行修補。
- 影響平台：
 - Splunk Enterprise 9.4.0 至 9.4.13、10.0.0 至 10.0.8、10.2.0 至 10.2.5 及 10.4.0 至 10.4.1 版本

- 資料來源：

1. [Security Hardening Release for Splunk Enterprise - August 2026](#)
2. [CVE-2026-76253](#)
3. [CVE-2026-76310](#)
4. [CVE-2026-76311](#)
5. [CVE-2026-76312](#)
6. [CVE-2026-76313](#)
7. [CVE-2026-76314](#)
8. [CVE-2026-76315](#)
9. [CVE-2026-76316](#)
10. [CVE-2026-76317](#)
11. [CVE-2026-76319](#)
12. [CVE-2026-76335](#)
13. [CVE-2026-76350](#)
14. [CVE-2026-76351](#)
15. [CVE-2026-76352](#)

2.3.4 Zimbra Collaboration存在高風險安全漏洞(CVE-2026-73570)，請儘速確認並進行修補

CVE 編號	CVE-2026-73570
影響產品	Zimbra Collaboration
解決辦法	官方已針對漏洞釋出修補程式，請升級 Zimbra Collaboration 至 10.1.20(含)以後版本。 詳細說明請參考官方公告，網址如下： https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

- 內容說明：
研究人員發現 Zimbra Collaboration 存在作業系統指令注入(OS Command Injection)漏洞(CVE-2026-73570)，當系統安裝選用套件 zimbra-snmp 並啟用 SNMP 通知功能時，未經身分鑑別之遠端攻擊者可藉由傳送特製 SMTP 請求，以 Zimbra 使用者權限執行任意作業系統指令。該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台：
 - Zimbra Collaboration 10.1.20(不含)以前版本
- 資料來源：
 1. [Zimbra Security Advisories](#)
 2. [Zimbra Collaboration Suite \(ZCS\) OS Command Injection Vulnerability](#)
 3. [CVE-2026-73570](#)

2.3.5 SonicWall NSM On-Prem 存在2個重大資安漏洞

CVE 編號	CVE-2026-78327,CVE-2026-81939
影響產品	SonicWall NSM On-Prem
解決辦法	請更新至以下版本： Network Security Manager (NSM) On-Prem 4.3.1-R4 (含)之後版本

- 內容說明：

SonicWall 針對 NSM On-Prem 發布重大資安漏洞(CVE-2026-78327，CVSS：9.1 和 CVE-2026-81939，CVSS：9.1)，CVE-2026-81939 為 Zip Slip 漏洞，存在於 NSM On-Prem 的檔案上傳與壓縮檔處理功能中，攻擊者可利用精心設計的檔案，將檔案解壓縮至預期目標目錄外；CVE-2026-78327 為作業系統命令注入漏洞，允許經身分驗證且具有 SuperAdmin 權限的攻擊者，在底層主機上執行任意命令，從而導致遠端程式碼執行。

- 影響平台：

- Network Security Manager (NSM) On-Prem 4.3.0 (含)以前版本

- 資料來源：

1. [SonicWall NSM On-Prem Affected By Multiple Vulnerabilities](#)

2.3.6 Cisco 旗下 Nexus 9000系列交換器存在重大資安漏洞(CVE-2026-20212)

CVE 編號	CVE-2026-20212
影響產品	Cisco Nexus 9000
解決辦法	根據官方網站釋出的解決方式進行修補

- 內容說明：

Cisco 針對旗下 Nexus 9000 系列交換器發布重大資安漏洞公告(CVE-2026-20212，CVSS：9.8)，Cisco Nexus 9000 系列交換器的 Silicon One 整合存在漏洞，可能允許未經身份驗證的遠端攻擊者以 root 權限執行程式碼。

- 影響平台：

- N9324C-SE1U
- N9348Y2C6D-SE1U
- N9364E-SG2-O
- N9364E-SG2-Q
- N9396T12C-SE1
- N9348Y12C-SE1
- N9396Y12C-SE1
- N9336C-SE1
- N9K-C9804
- N9K-C9808

- 資料來源：

1. [Cisco Nexus 9000 Series Switches Silicon One Remote Code Execution Vulnerability](#)
2. [CVE-2026-20212](#)

2.3.7 Cisco IOS XR Software 存在5個重大資安漏洞

CVE 編號	CVE-2026-20280,CVE-2026-20279,CVE-2026-20278,CVE-2026-20275,CVE-2026-20274
影響產品	Cisco IOS XR Software
解決辦法	根據官方網站釋出的解決方式進行修補。

- 內容說明：

Cisco IOS XR Software 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-2026-20280(CVSS：8.8)，為對異常情況檢查或處理不當。

CVE-2026-20279(CVSS：9.8)，為存取控制不當漏洞。

CVE-2026-20278(CVSS：8.8)，為不適當處理漏洞。

CVE-2026-20275(CVSS：8.8)，為計算錯誤，包含緩衝區大小計算錯誤、整數溢位等。

CVE-2026-20274(CVSS：9.8)，在資源的生命週期內對其進行不當控制。

- 影響平台：

- 詳細受影響產品清單與版本，請參閱官方網站公告。

- 資料來源：

1. [Cisco IOS XR Software Security Hardening Release: September 2026](#)
2. [CVE-2026-20274](#)
3. [CVE-2026-20275](#)
4. [CVE-2026-20278](#)
5. [CVE-2026-20279](#)
6. [CVE-2026-20280](#)

2.3.8 WatchGuard 旗下 Fireware OS iked 存在3個重大資安漏洞

CVE 編號	CVE-2026-19313,CVE-2026-19315,CVE-2026-19318
影響產品	WatchGuard Fireware OS iked
解決辦法	請更新至以下版本： 【CVE-2026-19313、CVE-2026-19318】 Default - Fireware OS 2026.2.2(含)之後版本、 Default - Fireware OS 12.12.2(含)之後版本、 T15/T35 - Fireware OS 12.5.20(含)之後版本、 T15/T35 - Fireware OS 2026.3.1(含)之後版本 【CVE-2026-19315】 Default - Fireware OS 2026.2.2(含)之後版本、 Default - Fireware OS 12.12.2(含)之後版本、 Default - Fireware OS 2026.3.1(含)之後版本 T15/T35 - Fireware OS 12.5.20(含)之後版本、

- 內容說明：

WatchGuard 針對旗下 Fireware OS iked 發布重大資安漏洞公告(CVE-2026-19313、CVE-2026-19315、CVE-2026-19318)，CVSS 4.x 評分皆為 9.3。

CVE-2026-19313，此為 heap 溢出漏洞，允許未經身分驗證的遠端攻擊者，利用精心設計的網路流量執行任意程式碼。

CVE-2026-19315，此為類型混淆漏洞，允許未經身分驗證的遠端攻擊者，利用特製的網路封包觸發記憶體處理錯誤，可能進一步執行任意程式碼。

CVE-2026-19318，此為 Stack-based Buffer Overflow (堆疊型緩衝區溢位)，允許未經身分驗證的遠端攻擊者，利用特製的網路封包執行任意程式碼。

- 影響平台：

- Default - Fireware OS 2025.0 至 2026.2.2(不含)版本
- Default - Fireware OS 12.0 至 12.12.2(不含)版本
- T15/T35 - Fireware OS 12.0 至 12.5.20(不含)版本
- T15/T35 - Fireware OS 2026.3 至 2026.3.1(不含)版本
- Default - Fireware OS 2026.3 至 2026.3.1(不含)版本

- 資料來源：

1. [Fireware OS Pre-Authentication Heap Buffer Overflow in iked Allows Remote Code Execution](#)
2. [Fireware OS Pre-Authentication Type Confusion in iked Allows Remote Code Execution](#)
3. [Fireware OS Pre-Authentication Stack Buffer Overflow in iked Allows Remote Code Execution](#)
4. [CVE-2026-19313](#)
5. [CVE-2026-19315](#)
6. [CVE-2026-19318](#)

2.3.9 Ivanti Neurons for ITSM存在8個高風險資安漏洞

CVE 編號	CVE-2026-12744,CVE-2026-12745,CVE-2026-12651,CVE-2026-12650,CVE-2026-12648,CVE-2026-12645,CVE-2026-12646,CVE-2026-12647
影響產品	Ivanti Neurons for ITSM
解決辦法	請更新至以下版本： Ivanti Neurons for ITSM (Cloud / SaaS) mo2026.2 (含)之後版本 Ivanti Neurons for ITSM On-Prem 2025.2 Sept 2026 Security Patch Ivanti Neurons for ITSM On-Prem2025.3 Sept 2026 Security Patch Ivanti Neurons for ITSM On-Prem2025.4 Sept 2026 Security Patch Ivanti Neurons for ITSM On-Prem2026.1 Sept 2026 Security Patch Ivanti Neurons for ITSM On-Prem (含)之後 2026.2 版本

- 內容說明：

ITSM 是 Ivanti 旗下一款可靠且強大 IT 服務管理的解決方案，可協助組織提升服務效率，確保 IT 營運合規及安全。近日針對 Ivanti Neurons for ITSM 發布重大資安公告，其產品存在 8 個高風險資安漏洞。

CVE-2026-12744 (CVSS : 9.8) 為不受信任資料反序列化漏洞，允許未經身分驗證的遠端攻擊者在伺服器上執行任意程式碼。

CVE-2026-12745 (CVSS : 9.8) 為不受信任資料反序列化漏洞，允許未經身分驗證的遠端攻擊者在伺服器上執行任意程式碼。

CVE-2026-12651 (CVSS : 8.8) 為不受信任資料反序列化漏洞，允許經身分驗證的遠端攻擊者在伺服器上執行任意程式碼。

CVE-2026-12650 (CVSS : 9.9) 為不受信任資料反序列化漏洞，允許經身分驗證的遠端攻擊者在伺服器上執行任意程式碼。

CVE-2026-12648 (CVSS : 8.8) 為不受信任資料反序列化漏洞，允許經身分驗證的遠端攻擊者在伺服器上執行任意程式碼。

CVE-2026-12645 (CVSS : 9.9) 為授權缺失漏洞，允許經身分驗證的遠端攻擊者在伺服器上執行任意程式碼。

CVE-2026-12646 (CVSS : 9.9) 為授權缺失漏洞，允許經身分驗證的遠端攻擊者在伺服器上執行任意程式碼。

CVE-2026-12647 (CVSS : 9.9) 為授權缺失漏洞，允許經身分驗證的遠端攻擊者在伺服器上執行任意程式碼。

- 影響平台：

- Ivanti Neurons for ITSM (Cloud / SaaS) 2026.2 版本
- Ivanti Neurons for ITSM On-Prem 2025.2 、 2025.3 、 2025.4 、 2026.1 版本

- 資料來源：

1. [Security Advisory Ivanti Neurons for ITSM \(Multiple CVEs\)](#)
2. [CVE-2026-12744](#)
3. [CVE-2026-12745](#)
4. [CVE-2026-12651](#)
5. [CVE-2026-12650](#)
6. [CVE-2026-12648](#)
7. [CVE-2026-12645](#)
8. [CVE-2026-12646](#)
9. [CVE-2026-12647](#)

2.3.10 Ivanti旗下Endpoint Manager Mobile (EPMM)存在重大資安漏洞(CVE-2026-18851)

CVE 編號	CVE-2026-18851
影響產品	Ivanti Endpoint Manager Mobile
解決辦法	請更新至以下版本： Ivanti Endpoint Manager Mobile 12.10.0.0(含)之後版本 Ivanti Endpoint Manager Mobile 12.9.0.2(含)之後版本 Ivanti Endpoint Manager Mobile 12.8.0.4(含)之後版本

- 內容說明：

Ivanti Endpoint Manager Mobile (EPMM)是一款移動設備管理解決方案，能集中管理 iOS、Android、macOS 和 Windows 設備，近日 Ivanti 發布重大資安漏洞公告(CVE-2026-18851，CVSS：8.8)，此為缺少授權漏洞，允許經身分驗證的遠端攻擊者能將自身權限提升至管理員。
- 影響平台：
 - Ivanti Endpoint Manager Mobile 12.9.0.1(含)之前版本
 - Ivanti Endpoint Manager Mobile 12.8.0.3(含)之前版本
- 資料來源：
 1. [Security Advisory - Ivanti Endpoint Manager Mobile \(CVE-2026-18851\)](#)
 2. [CVE-2026-18851](#)

2.3.11 Fortinet旗下FortiSandbox、FortiSandbox Cloud 和 FortiSandbox PaaS 存在重大資安漏洞(CVE-2026-26084)

CVE 編號	CVE-2026-26084
影響產品	Fortinet FortiSandbox、FortiSandbox Cloud、FortiSandbox PaaS
解決辦法	請更新至以下版本： FortiSandbox 5.0.6(含)之後版本 FortiSandbox 4.4.9(含)之後版本 FortiSandbox Cloud 5.0.6(含)之後版本 FortiSandbox PaaS 5.0.6(含)之後版本

- 內容說明：
Fortinet 旗下 FortiSandbox、FortiSandbox Cloud 和 FortiSandbox PaaS 的網頁介面存在缺少存取控制漏洞(CVE-2026-26084，CVSS：9.9)，允許未經身分驗證的攻擊者，透過特製的 HTTP 請求存取敏感資訊。
- 影響平台：
 - FortiSandbox 5.0.0 至 5.0.5 版本
 - FortiSandbox 4.4.0 至 4.4.8 版本
 - FortiSandbox Cloud 5.0.4 至 5.0.5 版本
 - FortiSandbox PaaS 5.0.4 至 5.0.5 版本
- 資料來源：
 1. [Unauthenticated Control of NAT Rules Leading to Exposure of Sensitive Information](#)
 2. [CVE-2026-26084](#)

2.3.12 Fortinet Privileged Access Agent Chrome Extension存在重大資安漏洞 (CVE-2026-84388)

CVE 編號	CVE-2026-84388
影響產品	Fortinet Privileged Access Agent Chrome Extension
解決辦法	請更新至以下版本： FortiPAM Chrome Extension 8.0.1.123(含)之後版本

- 內容說明：

Fortinet Privileged Access Agent Chrome Extension 存在不正確的身分驗證漏洞(CVE-2026-84388，CVSS：9.1)，若使用者造訪惡意網站，可能允許未經身分驗證的遠端攻擊者控制伺服器代理使用者的瀏覽器流量。

- 影響平台：

- FortiPAM Chrome Extension 8.0 所有版本
- FortiPAM Chrome Extension 7.4 所有版本

- 資料來源：

1. [Improper Authentication of FortiPAM Server](#)

2.3.13 FortiMonitorOnSight存在重大資安漏洞(CVE-2026-84390)

CVE 編號	CVE-2026-84390
影響產品	FortiMonitorOnSight
解決辦法	請更新至以下版本： FortiMonitorOnSight 7.2.8(含)之後版本

- 內容說明：

FortiMonitorOnSight Web 入口網站存在原始碼含有敏感資訊漏洞 (CVE-2026-84390，CVSS：9.6)，此漏洞可能允許未經身分驗證的遠端攻擊者，透過偽冒或重複使用 JWT 繞過身分驗證。
- 影響平台：
 - FortiMonitorOnSight 7.2.0 至 7.2.2 版本
 - FortiMonitorOnSight 7.2.4 至 7.2.7 版本
- 資料來源：
 1. [JWT used for authentication in web GUI signed with static key](#)

2.3.14 MikroTik RouterOS 存在3個重大資安漏洞

CVE 編號	CVE-2026-67276,CVE-2026-86060,CVE-2026-67277
影響產品	MikroTik RouterOS
解決辦法	請更新至以下版本： MikroTik RouterOS 7.25 beta3(含)之後版本 MikroTik RouterOS 7.24.2(含)之後版本 MikroTik RouterOS 7.23.4(含)之後版本 MikroTik RouterOS 6.49.21(含)之後版本

- 內容說明：

網路設備製造商 MikroTik 發布重大資安漏洞，路由器作業系統 RouterOS 存在 3 個重大資安漏洞。

CVE-2026-67276 (CVSS 4.x : 9.2)，RouterOS 在將 SSH 驗證請求與授權使用者金鑰比對時，不會比較完整 RSA 公鑰，而是檢查金鑰類型和模數，若攻擊者得知授權的 RSA 模數且偽造有效簽名，在沒有私鑰的情況下以目標用戶的身分開啟 SSH 命令通道。

CVE-2026-86060 (CVSS 4.x : 9.2)，RouterOS 的 SSH 登入路徑中存在一個參數處理漏洞，該漏洞涉及以停用字元開頭的使用者名，允許攻擊者更改受信任的 RouterOS 策略掩碼，從而導致權限提升。

CVE-2026-67277 (CVSS 4.x : 8.8)，RouterOS 完成身份驗證之前接受一個「related」btest session connection, 駭客可在未經身份驗證的用戶端可以利用此狀態啟動 IPv4 UDP 測試, 可能重啟 RouterOS。

- 影響平台：

- MikroTik RouterOS 7.24 至 7.24.2(不含)版本
- MikroTik RouterOS 7.9 至 7.23.4(不含)版本
- MikroTik RouterOS 7.0.0 至 7.23.4(不含)版本

- MikroTik RouterOS 6.0.0 至 6.49.21(不含)版本
- 資料來源：
 1. [September 2026 vulnerability](#)
 2. [Critical vulnerabilities in MikroTik RouterOS are being actively exploited.](#)
 3. [CVE-2026-67276](#)
 4. [CVE-2026-86060](#)
 5. [CVE-2026-67277](#)

2.3.15 Cisco Secure Email Gateway 存在重大資安漏洞(CVE-2026-76461)

CVE 編號	CVE-2026-76461
影響產品	Cisco Secure Email Gateway
解決辦法	請更新至以下版本： Cisco AsyncOS for Cisco Secure Email Gateway 15.5.5-014(含)之後版本、 Cisco AsyncOS for Cisco Secure Email Gateway 16.0.4-302(含)之後版本、 Cisco AsyncOS for Cisco Secure Email Gateway 16.5.0-780(含)之後版本

- 內容說明：

Cisco 針對旗下 Secure Email Gateway 發布重大資安漏洞公告(CVE-2026-76461，CVSS：9.8)。此漏洞允許未經身分驗證的遠端攻擊者，透過寄送內含惡意 SQL 指令的特製電子郵件，以 root 權限於底層作業系統遠端執行任意程式碼 (RCE)。

備註：目前 Cisco 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：

- Cisco AsyncOS for Cisco Secure Email Gateway 15.5(含)之前版本
- Cisco AsyncOS for Cisco Secure Email Gateway 16.0 版本
- Cisco AsyncOS for Cisco Secure Email Gateway 16.5 版本

- 資料來源：

1. [Cisco Secure Email Gateway SQL Injection Vulnerability](#)
2. [CVE-2026-76461](#)

2.3.16 SAP針對旗下多款產品發布重大資安公告

CVE 編號	CVE-2026-44756,CVE-2026-58240,CVE-2026-76969,CVE-2026-66768
影響產品	SAP 旗下多款產品
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/september-2026.html?isu_page=1

- 內容說明：

SAP 發布九月份例行更新，共修補 20 項漏洞，其中 4 項屬於高風險資安漏洞(CVE-2026-44756，CVSS：10.0、CVE-2026-58240，CVSS：9.8、CVE-2026-76969，CVSS：9.4 和 CVE-2026-66768，CVSS：9.0)。CVE-2026-44756，Extended Passport Protocol (EPP)處理庫中存在記憶體安全漏洞，在特定條件下，未經身分驗證的攻擊者可利用特製的網路請求，導致程式出現未定義行為並異常終止。

CVE-2026-58240，SAP NetWeaver Message Server 在註冊過程中對內部應用伺服器元件的真實性驗證不足，未經身分驗證的攻擊者若有網路存取權限，可能在應用環境中執行未經授權的操作。

CVE-2026-76969，@sap/cds-mtxs NPM library 對啟用可擴展性的 multitenant CAP 應用中使用的某些功能未進行充分檢查，未經身分驗證的攻擊者可利用特製的請求獲取敏感憑證。

CVE-2026-66768，SAP GUI for Java 對某些從連接的後端系統呼叫函數未能正確執行信任等級策略，低權限的攻擊者可利用此漏洞，透過操縱連接的後端系統導致在受害者機器上執行任意命令。

- 影響平台：

- SAP Extended Passport (EPP) Processing KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, 8.04, WEBDISP 9.16,

9.18, 9.19, 9.20, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04,
9.16, 9.18, 9.19, 9.20 版本

- SAP NetWeaver (Message Server) KERNEL 9.16, 9.18, 9.19, 9.20 版本
- sap/cds-mtxs <=1.18.3, <=2.7.6, <=3.9.6, <=4.0.2 版本
- SAP NetWeaver (SAP GUI for Java) BC-FES-JAV 8.10 版本

● 資料來源：

1. [SAP Security Patch Day - September 2026](#)
2. [CVE-2026-44756](#)
3. [CVE-2026-58240](#)
4. [CVE-2026-76969](#)
5. [CVE-2026-66768](#)

2.3.17 Check Point 旗下產品 Security Gateway、Security Management Server 與 Spark Firewall 存在 2 個重大資安漏洞

CVE 編號	CVE-2026-85102, CVE-2026-85103
影響產品	Check Point Security Gateway、Security Management Server、Spark Firewall
解決辦法	根據官方網站釋出的解決方式進行修補

- 內容說明：

Check Point 針對旗下產品 Security Gateway、Security Management Server 與 Spark Firewall 發布重大資安漏洞公告 (CVE-2026-85102, CVSS : 9.8 和 CVE-2026-85103, CVSS : 9.8)。

CVE-2026-85102, VPN 協商期間憑證資料驗證不當可能導致未經身分驗證的遠端攻擊者在 Security Gateway 執行任意程式碼。

CVE-2026-85103, 此為 heap 溢位漏洞, 存在於 VPN 憑證 ASN.1 解碼流程中, 可能允許遠端攻擊者在 management 和 Security Gateway 上遠端執行任意程式碼。

- 影響平台：

- Security Gateway, Spark Firewall (Centrally Managed), Spark Firewall (Locally Managed) R81 (EOS), R81.10 (EOS), R81.10.X, R81.10.X, R81.20, R82, R82.00.X, R82.00.X, R82.10
- Security Gateway, Security Management Server, Spark Firewall (Centrally Managed), Spark Firewall (Locally Managed) R81 (EOS), R81 (EOS), R81.10 (EOS), R81.10 (EOS), R81.10.X, R81.10.X, R81.20, R81.20, R82, R82, R82.00.X, R82.00.X, R82.10, R82.10

- 資料來源：
 1. [CVE-2026-85102 - Authentication Bypass and Remote Code Execution in Remote Access and Site-to-Site V](#)
 2. [CVE-2026-85103 - ASN.1 decoding heap overflow leading to a remote code execution](#)
 3. [CVE-2026-85102](#)
 4. [CVE-2026-85103](#)

2.3.18 Cisco Secure Email Gateway 和 Secure Email and Web Manager存在4個重大資安漏洞

CVE 編號	CVE-2026-76440,CVE-2026-76441,CVE-2026-20353,CVE-2026-76443
影響產品	Cisco Secure Email Gateway 、 Secure Email and Web Manager
解決辦法	請更新至以下版本： Cisco Secure Email Gateway 15.5.5-014(含)之後版本、 Cisco Secure Email Gateway 16.5.0-780(含)之後版本、 Cisco Secure Email and Web Manager 15.5.5-006(含)之後版本、 Cisco Secure Email and Web Manager 16.5.0-429(含)之後版本

- 內容說明：

Cisco Secure Email Gateway 和 Secure Email and Web Manager 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-2026-76440，CVSS：9.8，路徑遍歷，含路徑名未正確限制到受限目錄、文件訪問前連結解析不當。

CVE-2026-76441，CVSS：9.8，存取控制不當，含授權、認證、權限和繞過。

CVE-2026-20353，CVSS：9.8，在資源生命週期內，對資源的控制不當，含不受控制的資源消耗、演算法複雜度等。

CVE-2026-76443，CVSS：9.8，此為不適當處理漏洞。

- 影響平台：

- Cisco Secure Email Gateway 15.5(含)之前版本
- Cisco Secure Email Gateway 16.0 版本

- Cisco Secure Email Gateway 16.5 版本
- Cisco Secure Email and Web Manager 15.5(含)之前版本
- Cisco Secure Email and Web Manager 16.0 版本
- Cisco Secure Email and Web Manager 16.5 版本
- 資料來源：
 1. [Cisco Secure Email Gateway and Secure Email and Web Manager Security Hardening Release: September 20](#)
 2. [CVE-2026-76440](#)
 3. [CVE-2026-76441](#)
 4. [CVE-2026-76443](#)
 5. [CVE-2026-20353](#)

2.3.19 Microsoft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	Microsoft 旗下多款產品
解決辦法	根據官方網站釋出的解決方式進行修補 https://msrc.microsoft.com/update-guide/releaseNote/2026-Sep

- 內容說明：

Microsoft 釋出 115 年 9 月份安全性更新，共修補 978 個漏洞，其中包含 193 個高風險漏洞與 2 個漏洞(CVE-2026-85880、CVE-2026-81963)已遭利用，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. [2026 年 9 月安全性更新](#)

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	 國家資通安全研究院- 產業資安職能訓練 資安事件應變 工程師 115002期 115/10/19~10/23 【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>



課程結束通過考核將獲得國家資通安全研究院及國立中興大學聯名頒發滲透測試工程師結訓證書乙張

培訓時間：115年11月07日至12月05日，每週六9:00-16:00，共30小時
報名費用：新台幣30,000元
洽詢單位：國立中興大學 創新產業暨國際學院企劃行銷組 (綜合教學大樓8樓802室) 04-22855506 朱小姐
國家資通安全研究院 02-23800912 方小姐

課程目標：
具備辨識漏洞、執行漏洞評估、風險分級管理之能力，並提出可行且有效的補救與強化建議報告

報名連結
QR Code

社交媒體：@iciilpm, nchuiii, nchuiii

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	
弱點掃描與漏洞修補	
活動時間	2026年 10 月 05 日 (一) 09:00 - 17:30
活動地點	台南市歸仁區歸仁13路一段6號 (數位產業署沙崙資安服務基地-1樓 攻防教室C115室)
活動網站	https://ievents.iii.org.tw/EventS.aspx?t=0&id=3458
活動概要	【費用】 免費 報名截止：2026/10/04 【課程目的】 本課程將協助學員了解弱點掃描與漏洞修補之核心觀念，探討 AI 於漏洞分析、風險評估及安全檢測之應用方向，並介紹生成式 AI 相關安全風險與防護重點。透過案例解析與實務操作，協助學員掌握弱點管理流程與應用安全觀念，提升企業資安防護與風險管理能力。 【課程講師】博創資訊股份有限公司 劉育彰 顧問 【課程對象】資安工程師、網管人員、系統維運人員、軟體開發人員、資訊 / 資安相關從業人員 【聯絡窗口】(06)3032260#529 田小姐 yztien@iii.org.tw
資安健檢與風險量化評估	
活動時間	2026年 10 月 13 日 (二) 09:00 - 17:30
活動地點	台南市歸仁區歸仁13路一段6號 (數位產業署沙崙資安服務基地-1樓 攻防教室C115室)
活動網站	https://ievents.iii.org.tw/EventS.aspx?t=0&id=3459
	【費用】 免費 報名截止：2026/10/08

活動概要	【課程目的】 本課程將介紹資安健檢與風險量化評估之核心觀念，協助學員了解如何透過資產盤點、風險識別及量化分析方法，掌握組織面臨之資安風險，並建立風險量化評估機制，作為資安治理與決策規劃之參考依據。 【課程講師】 曾子維 維域智慧執行長 【課程對象】 網管人員、資安工程師、IT 團隊主管 【聯絡窗口】 (06)3032260#529 田小姐 yztien@iii.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
活動概要	【費用】 原價：8,500元/人 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：

旭辰資訊 SmartIT Desktop Manager - 存在2個漏洞	
TVN / CVE ID	TVN-202609001 / CVE-2026-85146, CVE-2026-85148
CVSS	【CVE-2026-85146】 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 【CVE-2026-85148】 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	SmartIT Desktop Manager 10(含)以前版本
問題描述	【CVE-2026-85146(Use of Hard-coded Credentials)】 未經身分鑑別之遠端攻擊者可於程式碼中取得 SmartIT Agent 程式之 SSH 服務帳號與通行碼。 【CVE-2026-85148(Use of Hard-coded Credentials)】 未經身分鑑別之遠端攻擊者可利用固定通行碼遠端存取使用者主機。
解決方法	更新至 SmartIT Desktop Manager 11(含)以後版本
公開日期	2026-09-04
相關連結	https://www.twcert.org.tw/tw/cp-132-11176-a4cc2-1.html
英特內 DreamMaker - SQL Injection	
TVN / CVE ID	TVN-202609002 / CVE-2026-85540
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	Dreammaker

問題描述	【CVE-2026-85540(SQL Injection)】 已通過身分鑑別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	針對自行開發的功能，資料庫查詢或異動功能時，建議統一使用系統既有的 SQLBuilder 元件進行 SQL 組合、參數處理及資料庫操作。 應避免直接將外部輸入資料、表單參數或 URL 參數以字串串接方式組成 SQL 指令，以降低因自行開發程式處理不當而產生 **SQL Injection (SQL 注入) **弱點的風險。 透過 SQLBuilder 或其他具備參數化查詢機制的標準元件，可進一步強化輸入資料處理及 SQL 執行安全性，並降低應用程式受到惡意 SQL 指令注入攻擊的可能性，相關元件開發使用手冊可洽本公司客服系統。
公開日期	2026-09-04
相關連結	https://www.twcert.org.tw/tw/cp-132-11183-06a5e-1.html
昊亞科技 WeenyGenius - 存在3個漏洞	
TVN / CVE ID	TVN-202609005 / CVE-2026-89176, CVE-2026-89177, CVE-2026-89178
CVSS	【CVE-2026-89176】 8.8 (High) CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 【CVE-2026-89177】 8.8 (High) CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 【CVE-2026-89178】 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	WeenyGenius 12.2.031(含)以前版本

問題描述	【CVE-2026-89176(Missing Authentication)】 未經身分鑑別之同網域攻擊者可輕易冒用學生或教師電腦，若冒用學生可影響學生課堂正常使用，冒用老師則可控制學生電腦。 【CVE-2026-89177(Use of Insecure Protocol)】 由於通訊協定採用ZMTP Null模式，未經身分鑑別之同網域攻擊者可側錄監聽封包以取得傳輸內容。 【CVE-2026-89178(Origin Validation Error)】 未經身分鑑別之同網域攻擊者可偽冒老師端發起廣播封包，使學生端電腦嘗試與攻擊者建立連線。
解決方法	更新至 12.3.033(含)以後版本
公開日期	2026-09-11
相關連結	https://www.twcert.org.tw/tw/cp-132-11201-658c0-1.html
恒基科技 OAKlouds - Insecure Deserialization	
TVN / CVE ID	TVN-202609008 / CVE-2026-93467
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	OAKlouds-custom_page-2.0 26(不含)以前版本 OAKlouds-custom_page-3.0 26(不含)以前版本 OAKlouds-custom_page-4.0 26(不含)以前版本
問題描述	【CVE-2026-93467(Insecure Deserialization)】 未經身分鑑別之遠端攻擊者可透過發送惡意序列化內容於伺服器端執行任意程式碼。
解決方法	更新OAKlouds-custom_page-2.0至26(含)以後版本 更新OAKlouds-custom_page-3.0至26(含)以後版本

	更新OAKlouds-custom_page-4.0至26(含)以後版本
公開日期	2026-09-18
相關連結	https://www.twcert.org.tw/tw/cp-132-11210-11cb0-1.html
全景軟體 CGServiSign - OS Command Injection	
TVN / CVE ID	TVN-202609009 / CVE-2026-15027
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	Linux版NHIServisign_1.0.23.1227 版本
問題描述	全景軟體開發之CGServiSign存在OS Command Injection漏洞，未經身分鑑別之遠端攻擊者可誘導受害者瀏覽惡意網頁，注入任意作業系統指令並於受害者本機電腦上執行。
解決方法	請更新Linux版NHIServisign_1.0.26.0625(含)以上
公開日期	2026-09-23
相關連結	https://www.twcert.org.tw/tw/cp-132-11213-28a81-1.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/>