TWCERT/CC 資安情資電子報

2026 年 3 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

開源漏洞掃描工具 Trivy 遭 TeamPCP 供應鏈攻擊，恐導致CI/CD 機敏資料外洩

由雲端資安廠商Aqua Security 維護的知名開源漏洞掃描工具 Trivy，近期證實遭名為 TeamPCP的駭客組織發動大規模供應鏈攻擊。攻擊者利用未完全撤銷的高權限服務帳號憑證，成功竄改 Trivy 官方發布版本及 GitHub Actions，並將惡意竊資軟體植入CI/CD流程中，導致惡意蠕蟲在npm套件庫中大規模擴散。

根據資安研究人員與Aqua Security 的研究調查，此次事件源於2026年2月底 CI/CD環境配置不當導致高權限存取Token外洩。儘管官方於3

月1日進行憑證輪替，但因處理不全，駭客仍保有部分存取權限。3月19日，駭客利用殘留憑證對aquasecurity/trivy-action 儲存庫發動「強制推送(Force-push)」，竄改 76 個版本標籤中的75個，以及setup-trivy的7個版本標籤。導致特定版本標籤的CI/CD流程在不知情的狀況下執行惡意程式碼。此外，駭客還在 Docker Hub 上發布包含惡意程式碼的 Trivy 映像檔（0.69.4、0.69.5 與 0.69.6版本）。

此次攻擊植入的惡意程式為「TeamPCP Cloud stealer」，該程式針對GitHub Actions 的執行環境進行記憶體與檔案系統掃描，竊取AWS、GCP、Azure等雲端憑證、SSH 金鑰、Kubernetes Token、Docker 設定及多種加密貨幣錢包等機敏資料。竊得的資料會被加密並外傳至駭客控制的C2（scan.aquasecurtiy[.]org）；若傳輸失敗，惡意程式還會利用受害者環境中的 GitHub Token，在受害者帳號下建立名為 tpcp-docs 的公開儲存庫來存放外洩資料。

這起供應鏈攻擊的後續影響極為廣泛且具破壞性，駭客利用竊取的npm 發布Token，將名為「CanisterWorm」的自我繁殖蠕蟲植入超過 47個npm套件中，使得安裝這些套件的開發者可能成為下一個傳播節點。目前，Aqua Security 已將遭到竄改的惡意版本與映像檔移除，並聲明其商業版產品並未受到此次事件影響。

資安專家呼籲，曾於3月19日至20日期間使用過受影響版本的開發團隊，應將所有相關 CI/CD 流程中的憑證視為已遭外洩，並採取以下防護與應對措施：

- 將 Trivy 執行檔退回或更新至確認安全的 v0.69.2 或 v0.69.3；將 trivy-action 更新至未受影響的 v0.35.0；將 setup-trivy 更新至 v0.2.6。

- 立即撤銷並重新核發所有可能暴露在受影響 CI/CD 流程中的機密資訊，包含雲端供應商憑證、SSH 金鑰、Kubernetes Token 以及 npm 發布 Token等。
- 檢查企業/組織內是否出現名為tpcp-docs 的異常儲存庫，並在防火牆阻擋惡意網域 scan.aquasecurtiy[.]org 及 IP 位址 45[.]148.10.212。
- GitHub Actions 工作流程中，應使用完整的Commit SHA 雜湊值鎖定版本，而非使用易被竄改的Tag 標籤，以防範未來的供應鏈攻擊。

以下是針對此次供應鏈攻擊的IoC資訊：

scan[.]aquasecurtiy[.]org
45.148.10.212
18a24f83e807479438dcab7a1804c51a00dafc1d526698a66e0640d1e5dd671a
f7084b0229dce605ccc5506b14acd4d954a496da4b6134a294844ca8d601970d
822dd269ec10459572dfaaefe163dae693c344249a0161953f0d5cdd110bd2a0
e64e152afe2c722d750f10259626f357cdea40420c5eedae37969fbf13abbecf

- 相關連結

1. opensourcemalware-trivy
2. Trivy Under Attack Again: Widespread GitHub Actions Tag Compromise Exposes CI/CD Secrets
3. Trivy Supply Chain Attack Expands to Compromised Docker Images
4. Trivy Compromised: Everything You Need to Know about the Latest Supply Chain Attack
5. Update: Ongoing Investigation and Continued Remediation
6. From Scanner to Stealer: Inside the trivy-action Supply Chain Compromise
7. Trivy Security Scanner GitHub Actions Breached, 75 Tags Hijacked to Steal CI/CD Secrets
8. Trivy Supply Chain Attack Triggers Self-Spreading CanisterWorm Across 47 npm Packages
9. Trivy Hack Spreads Infostealer via Docker, Triggers Worm and Kubernetes Wiper

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 新型惡意軟體 KadNap 鎖定家用路由器

資安研究團隊 Black Lotus Labs 近期發現一款名為「KadNap」的新型惡意軟體，該威脅自2025年8月起活躍，主要針對多家知名品牌邊緣網路設備(edge device)與家用(SOHO)路由器進行攻擊。遭感染的設備會被納入殭屍網路，並成為非法代理服務「Doppelganger」的一部分，供網路犯罪者利用。目前全球估計超過14,000台設備受害，受影響地區主要集中於美國(60%)，台灣、香港與俄羅斯亦有約5%的感染比例。

根據分析報告，KadNap展現高度隱匿性與技術性。攻擊者首先從IP位址為212.104.140[.]140的伺服器下載名為「aic.sh」的惡意腳本並透過建立排程任務（cron job）每小時定期執行以確保持續性。隨後下載名為

「kad」的惡意執行檔部署惡意軟體，該惡意軟體會強制關閉標準的SSH連接埠（Port 22）以防範外部管理介入並強化控制權。

KadNap採用客製化的Kademlia 分散式雜湊表（DHT）協定，這種點對點（P2P）技術能將指令與控制（C2）伺服器的 IP 位址隱藏在正常的 P2P 網路流量中，從而規避傳統的網路監控，大幅增加資安人員偵測與阻斷的難度。然而，資安專家發現，該軟體在連線到C2伺服器前會經過特定跳板節點(45.135.180[.]38 與 45.135.180[.]177)，此資訊可用於防火牆阻斷參考。

為防範邊緣網路設備與路由器遭KadNap或類似惡意軟體攻擊，建議採取以下防護措施：

- 定期更新韌體：確保路由器韌體維持在最新版本，以修補已知的安全漏洞。
- 強化帳號管理：切勿使用出廠預設密碼，應設定具備高強度(結合大小寫字母、數字與符號)的複雜密碼。
- 關閉遠端管理功能：確保路由器的管理介面(Web UI)未暴露於公開網路，關閉不必要的WAN端存取權限。
- 汰換過時設備：若設備已達生命週期終點(End-of-Life, EOL)，原廠不再提供安全更新與技術支援，請務必更換為受支援的設備。

以下是由資安研究團隊 Black Lotus Labs所提供的IoC：

85[.]158[.]111[.]100
89[.]46[.]38[.]74
154[.]7[.]253[.]12
212[.]104[.]141[.]88

91[.]193[.]19[.]226

79[.]141[.]161[.]152

91[.]193[.]19[.]51

79[.]141[.]163[.]155

23[.]227[.]203[.]221

45[.]135[.]180[.]38

45[.]135[.]180[.]177

0b3dbb951de7a216dd5032d783ba7d0a5ecda2bf872643c3a4ddd1667fb38ffe

ebf9de6b67e94b2bd2b0dcda1941e04fef1a1dad830404813e468ab8744b7ed8

- 相關連結

1. Silence of the hops: The KadNap botnet
2. Lumen_Github_KadNap_IOCs.txt
3. KadNap Malware Infects 14,000+ Edge Devices to Power Stealth Proxy Botnet
4. New KadNap botnet hijacks ASUS routers to fuel cybercrime proxy network

2.2 軟硬體系統資安議題

2.2.1 Interlock 勒索軟體組織利用 Cisco FMC 零日漏洞發動攻擊，呼籲用戶儘速修補

Amazon 威脅情報團隊發現，勒索軟體組織Interlock正積極利用 Cisco Secure Firewall Management Center (FMC) 的重大零日漏洞 (CVE-2026-20131，CVSS：10.0) 發動大規模攻擊。該漏洞屬於Java反序列化漏洞，允許未經身分驗證的遠端攻擊者，透過發送精心設計的反序列化物件，取得 root 最高權限並在受害設備上執行任意程式碼。建議用戶儘速依循Cisco官方建議，採取相關緩解措施並立即更新，同時檢視系統日誌確認潛在受害情形，以防止系統遭入侵後造成重大損失。

美國網路安全與基礎設施安全局（CISA）已正式將CVE-2026-20131納入已知漏洞目錄(KEV)，確認該漏洞正受到積極且廣泛的利用。根據Amazon 全球誘餌網路 (MadPot) 的監測數據顯示，在Cisco 正式發布修補

程式前，Interlock勒索軟體組織自 2026 年 1 月 26 日起便已將其作為零日漏洞進行「武器化」攻擊，防禦的空窗期長達 36 天。

研究報告顯示，資安研究人員透過攻擊者設定錯誤的伺服器，揭露其完整的攻擊工具與多階段攻擊流程，內容包含自訂後門、偵察工具及規避偵測手法，顯示其行動具有高度專業化特徵。

- 攻擊者除使用以JavaScript與Java開發的客製化RAT維持遠端控制外，並部署駐留在記憶體中的WebShell。此類無檔案手法可避免惡意程式落地，並透過攔截HTTP請求與執行加密載荷，提高規避偵測能力。
- 為了確保長期控制受害環境，攻擊者除部署合法的遠端連線工具ConnectWise ScreenConnect作為備用管道外，也利用Volatility(記憶體鑑識工具)等工具蒐集敏感資訊，並透過Certify濫用Active Directory憑證服務，以利進行滲透與權限提升。
- 攻擊者將Linux伺服器配置為HTTP反向代理以隱藏來源，並設定排程工作每五分鐘自動刪除系統日誌，藉此隱藏攻擊來源並阻礙資安人員的鑑識調查。

針對此次零日漏洞威脅，資安專家建議企業和組織立即採取以下防護措施：

- 受影響用戶應立即下載 Cisco 針對 Secure Firewall Management Center 釋出的安全性更新程式。
- 技術團隊應優先檢視系統日誌，檢查是否有未經授權的 ScreenConnect 安裝紀錄、異常連接埠（如 TCP 45588）連線，或 Java ServletRequestListener的異常註冊活動。

- 鑑於零日漏洞的不可預測性，企業應建立多層次安全控制與持續性監控機制。確保在單一節點遭突破時，仍具備後續層次的防禦能力，以最大程度縮減防禦空窗期的風險。

以下是由AWS所提供的IoC：

206.251.239[.]164
199.217.98[.]153
89.46.237[.]33
144.172.94[.]59
199.217.99[.]121
188.245.41[.]78
144.172.110[.]106
95.217.22[.]175
37.27.244[.]222
cherryberry[.]click
ms-server-default[.]com
initialize-configs[.]com
ms-global.first-update-server[.]com
ms-sql-auth[.]com
kolonialeru[.]com
sclair.it[.]com
browser-updater[.]com
browser-updater[.]live
os-update-server[.]com
os-update-server[.]org
os-update-server[.]live
os-update-server[.]top
d1caa376cb45b6a1eb3a45c5633c5ef75f7466b8601ed72c8022a8b3f6c1f3be
6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f

- 相關連結

1. Amazon threat intelligence teams identify Interlock ransomware campaign targeting enterprisefirewall
2. Interlock Ransomware Exploits Cisco FMC Zero-Day CVE-2026-20131 for Root Access
3. Interlock group exploiting the CISCO FMC flaw CVE-2026-20131 36 days before disclosure

2.3 軟硬體漏洞資訊

2.3.1 BeyondTrust Remote Support (RS)與Privileged Remote Access (PRA)存在重大資安漏洞(CVE-2026-1731)

CVE 編號	CVE-2026-1731
影響產品	BeyondTrust Remote Support、Privileged Remote Access
解決辦法	根據官方網站釋出的解決方式進行修補： https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

- 內容說明：

  BeyondTrust 針對旗下 BeyondTrust Remote Support (RS)與 Privileged Remote Access (PRA)發布重大資安漏洞公告(CVE-2026-1731，CVSS 4.x：9.9)，此漏洞允許未經身分驗證的遠端攻擊者可注入任意作業系統指令並於伺服器上執行。

  備註：目前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：
  - Remote Support 25.3.1(含)以前版本
  - Privileged Remote Access 24.3.4(含)以前版本
- 資料來源：
  1. BeyondTrust BT26-02
  2. CVE-2026-1731

2.3.2 Dell RecoverPoint for Virtual Machines存在重大資安漏洞(CVE-2026-22769)

CVE 編號	CVE-2026-22769
影響產品	Dell RecoverPoint for Virtual Machines
解決辦法	根據官方網站釋出的解決方式進行修補： https://www.dell.com/support/kbdoc/zh-tw/000426773/dsa-2026-079

- 內容說明：

  Dell RecoverPoint for Virtual Machines 存在使用硬編碼之帳號通行碼(Use of Hard-coded Credentials)漏洞(CVE-2026-22769，CVSS：10.0)，此漏洞允許未經身分認證的遠端攻擊者可使用硬編碼之帳號通行碼取得底層作業系統之 root 權限。

  備註：目前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：
  - RecoverPoint for Virtual Machines 5.3 SP4 P1(含)以前版本、6.0、6.0 SP1、6.0 SP1 P1、6.0 SP1 P2、6.0 SP2、6.0 SP2 P1、6.0 SP3 及 6.0 SP3 P1 版本
- 資料來源：
  1. DELL Technologies DSA-2026-079
  2. CVE-2026-22769

2.3.3 Junos OS Evolved PTX系列存在重大資安漏洞(CVE-2026-21902)

CVE 編號	CVE-2026-21902
影響產品	Junos OS Evolved PTX 系列產品
解決辦法	請更新至以下版本： Junos OS Evolved PTX 系列 25.4R1-S1-EVO、25.4R2-EVO、26.2R1-EVO(含)之後版本

- 內容說明：

  Juniper Networks 針對旗下 Junos OS Evolved PTX 系列產品發布重大資安公告(CVE-2026-21902，CVSS：9.8)，此為關鍵資源權限分配錯誤漏洞，允許未經身分驗證的攻擊者以 root 身分執行程式碼。

- 影響平台：
  - Junos OS Evolved PTX 系列 25.4R1-S1-EVO、25.4R2-EVO 版本
- 資料來源：
  1. JUNIPER 2026-02 Out-of-Cycle Security Bulletin
  2. CVE-2026-21902

2.3.4 Cisco Catalyst SD-WAN 存在3個重大資安漏洞

CVE 編號	CVE-2026-20127,CVE-2026-20126,CVE-2026-20129
影響產品	Cisco Catalyst SD-WAN
解決辦法	請更新至以下版本： 【CVE-2026-20127】 Cisco Catalyst SD-WAN 20.9.8.2(含)之後版本 Cisco Catalyst SD-WAN 20.12.6.1(含)之後版本 Cisco Catalyst SD-WAN 20.12.5.3(含)之後版本 Cisco Catalyst SD-WAN 20.12.6.1(含)之後版本 Cisco Catalyst SD-WAN 20.15.4.2(含)之後版本 Cisco Catalyst SD-WAN 20.18.2.1(含)之後版本 【CVE-2026-20126、CVE-2026-20129】 Cisco Catalyst SD-WAN Manager 20.9.8.2(含)之後版本 Cisco Catalyst SD-WAN Manager 20.12.6.1(含)之後版本 Cisco Catalyst SD-WAN Manager 20.12.5.3(含)之後版本 Cisco Catalyst SD-WAN Manager 20.12.6.1(含)之後版本 Cisco Catalyst SD-WAN Manager 20.15.4.2(含)之後版本 Cisco Catalyst SD-WAN Manager 20.15.4.2(含)之後版本 Cisco Catalyst SD-WAN Manager 20.18.2.1(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，近日 Cisco 發布重大資安公告。

  【CVE-2026-20127，CVSS：10.0】

此漏洞存在於 Cisco Catalyst SD-WAN Controller(formerly vSmart) 可能被未經身分驗證的遠端攻擊者利用，以繞過身分驗證機制並取得受影響系統的管理權限。

【CVE-2026-20126，CVSS：8.8】

此漏洞存在於 Cisco Catalyst SD-WAN Manager(formerly vManage) ，可能允許已通過身分驗證且具有本機低權限的攻擊者，利用 REST API 發送請求後，取得底層作業系統的 root 權限。

【CVE-2026-20129，CVSS：9.8】

此漏洞存在於 Cisco Catalyst SD-WAN Manager 的 API 使用者驗證，允許未經身分驗證的遠端攻擊者利用精心設計的 API 請求，以 netadmin 角色使用者的身分存取受影響的系統。

註：Cisco Catalyst SD-WAN Controller (formerly vSmart) 與 Cisco Catalyst SD-WAN Manager (formerly vManage) 已被發現積極利用於攻擊活動，請儘速採取應變措施。

- 影響平台：

【CVE-2026-20127】

- Cisco Catalyst SD-WAN 20.9 版本
- Cisco Catalyst SD-WAN 20.11 版本
- Cisco Catalyst SD-WAN 20.12.5 版本
- Cisco Catalyst SD-WAN 20.12.6 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

【CVE-2026-20126、CVE-2026-20129】

- Cisco Catalyst SD-WAN Manager 20.9 版本
- Cisco Catalyst SD-WAN Manager 20.11 版本

- Cisco Catalyst SD-WAN Manager 20.12.5 版本
- Cisco Catalyst SD-WAN Manager 20.12.6 版本
- Cisco Catalyst SD-WAN Manager 20.13 版本
- Cisco Catalyst SD-WAN Manager 20.14 版本
- Cisco Catalyst SD-WAN Manager 20.15 版本
- Cisco Catalyst SD-WAN Manager 20.16 版本
- Cisco Catalyst SD-WAN Manager 20.18 版本

- 資料來源：
  1. Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability
  2. Cisco Security Advisory Cisco Catalyst SD-WAN Vulnerabilities
  3. CVE-2026-20126
  4. CVE-2026-20127
  5. CVE-2026-20129

2.3.5 SolarWinds旗下Serv-U軟體存在4個重大資安漏洞

CVE 編號	CVE-2025-40538,CVE-2025-40539,CVE-2025-40540,CVE-2025-40541
影響產品	SolarWinds Serv-U
解決辦法	請更新至以下版本： SolarWinds Serv-U 15.5.4(含)之後版本

- 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 4 個重大資安漏洞。

  【CVE-2025-40538，CVSS：9.1】

  此為存取控制漏洞，允許攻擊者建立系統管理員，並透過網域管理員或群組管理員權限，以特權帳號身分執行任意程式碼。

  【CVE-2025-40539，CVSS：9.1】

  此為類型混淆漏洞，允許攻擊者能以特權帳號身分執行任意本機程式碼。

  【CVE-2025-40540，CVSS：9.1】

  此為類型混淆漏洞，允許攻擊者能以特權帳號身分執行任意本機程式碼。

  【CVE-2025-40541，CVSS：9.1】

  此為不安全直接物件參考(IDOR)漏洞，允許攻擊者能以特權帳號身分執行任意本機程式碼。

- 影響平台：
  - SolarWinds Serv-U 15.5 版本

- 資料來源：
  1. SolarWinds Serv-U Broken Access Control Remote Code Execution Vulnerability (CVE-2025-40538)
  2. SolarWinds Serv-U Type Confusion Remote Code Execution Vulnerability (CVE-2025-40539)
  3. SolarWinds Serv-U Type Confusion Remote Code Execution Vulnerability (CVE-2025-40540)
  4. SolarWinds Serv-U Insecure Direct Object Reference (IDOR) Remote Code Execution Vulnerability
  5. CVE-2025-40538
  6. CVE-2025-40539
  7. CVE-2025-40540
  8. CVE-2025-40541

2.3.6 n8n存在4個重大資安漏洞

CVE 編號	CVE-2026-27495,CVE-2026-27493,CVE-2026-27577,CVE-2026-27498
影響產品	n8n
解決辦法	【CVE-2026-27495、CVE-2026-27493、CVE-2026-27577】 請更新至以下版本： n8n 1.123.22(含)之後版本 n8n 2.9.3(含)之後版本 n8n 2.10.1(含)之後版本 【CVE-2026-27498】 請更新至以下版本： n8n 1.123.8(含)之後版本 n8n 2.2.0(含)之後版本

- 內容說明：

  n8n 是一款開源工作流程自動化工具，透過視覺化拖拉介面串接多種應用程式，無需程式碼即可自動化重複性任務，近日 n8n 發布重大資安公告。

  【CVE-2026-27495，CVSS：9.4】

  此漏洞允許經身分驗證且擁有或修改工作流程權限的攻擊者，可利用 JavaScript 任務執行沙箱中的漏洞，在邊界之外執行任意程式碼。

  【CVE-2026-27493，CVSS：9.5】

  此為二階段表達式注入漏洞，未經身分驗證的攻擊者，可透過精心設計的表單資料注入並執行任意 n8n 表達式，若與表達式的沙箱逃逸機制結合使用，可能導致在 n8n 主機上執行遠端程式碼。

  【CVE-2026-27577，CVSS：9.4】

此漏洞允許經身分驗證且擁有建立或修改工作流程權限的攻擊者，可利用特製的工作流程參數表達式，在執行 n8n 主機上觸發未經授權的系統指令。

【CVE-2026-27498，CVSS：9.0】

此漏洞允許經身分驗證且擁有建立或修改工作流程權限的攻擊者，利用 git 操作連結「從磁碟讀取/寫入檔案」節點，導致攻擊者可遠端程式碼執行。

- 影響平台：

【CVE-2026-27495、CVE-2026-27493、CVE-2026-27577】

- n8n 1.123.22(不含)之前版本
- n8n 2.0.0 至 2.9.3(不含)之前版本
- n8n 2.10.0 至 2.10.1(不含)之前版本

【CVE-2026-27498】

- n8n 1.123.8(不含)之前版本
- n8n 2.2.0(不含)之前版本

- 資料來源：

1. Sandbox Escape in JavaScript Task Runner
2. Unauthenticated Expression Evaluation via Form Node
3. Expression Sandbox Escape Leading to RCE
4. Arbitrary Command Execution via File Write and Git Operations
5. CVE-2026-27495
6. CVE-2026-27493
7. CVE-2026-27577
8. CVE-2026-27498

2.3.7 Microsoft Windows與Office存在5個高風險安全漏洞

CVE 編號	CVE-2026-21510,CVE-2026-21513,CVE-2026-21514,CVE-2026-21519,CVE-2026-21533
影響產品	Microsoft Windows 與 Office
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21510 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21514 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21519 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533

- 內容說明：

  研究人員發現 Microsoft Windows 與 Office 存在 5 個高風險安全漏洞，類型包含安全功能繞過(Security Feature Bypass)漏洞(CVE-2026-21510、CVE-2026-21513 及 CVE-2026-21514)與本機提權(Local Privilege Escalation)漏洞(CVE-2026-21519 與 CVE-2026-21533)，前者可使未經身分鑑別之攻擊者於使用者互動情境下繞過系統安全機制；後者可使已通過身分鑑別之攻擊者在既有權限基礎上提升權限。以上漏洞皆已遭駭客利用，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 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
- Microsoft Office LTSC for Mac 2021
- Microsoft Office LTSC for Mac 2024
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 24H2 for ARM64-based Systems
- Windows 11 Version 24H2 for x64-based Systems
- Windows 11 Version 25H2 for ARM64-based Systems
- Windows 11 Version 25H2 for x64-based Systems
- Windows 11 Version 26H1 for ARM64-based Systems
- Windows 11 Version 26H1 for x64-based Systems
- Windows Server 2012
- Windows Server 2012(Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2(Server Core installation)
- Windows Server 2016
- Windows Server 2016(Server Core installation)
- Windows Server 2019
- Windows Server 2019(Server Core installation)
- Windows Server 2022

- Windows Server 2022(Server Core installation)
- Windows Server 2022, 23H2 Edition(Server Core installation)
- Windows Server 2025
- Windows Server 2025(Server Core installation)

- 資料來源：
  1. CVE-2026-21510
  2. CVE-2026-21513
  3. CVE-2026-21514
  4. CVE-2026-21519
  5. CVE-2026-21533
  6. Windows Shell 安全性功能略過弱點
  7. MSHTML Framework Security Feature Bypass Vulnerability
  8. Microsoft Word 安全性功能略過弱點
  9. 桌面 Windows 管理員權限提高弱點
  10. Windows 遠端桌面服務權限提高弱點

2.3.8 以Chromium為基礎之瀏覽器存在高風險安全漏洞(CVE-2026-2441)

CVE 編號	CVE-2026-2441
影響產品	Chromium 為基礎之瀏覽器
解決辦法	請更新 Google Chrome 瀏覽器至 145.0.7632.75(含)以後版本 https://support.google.com/chrome/answer/95414?hl=zh-Hant 請更新 Microsoft Edge 瀏覽器至 144.0.3719.130 或 145.0.3800.58(含)以後版本 https://support.microsoft.com/zh-tw/topic/microsoft-edge-%E6%9B%B4%E6%96%B0%E8%A8%AD%E5%AE%9A-af8aaca2-1b69-4870-94fe-18822dbb7ef1 請更新 Vivaldi 瀏覽器至 7.8.3925.73 (含)以後版本 https://help.vivaldi.com/desktop/install-update/update-vivaldi/ 請更新 Brave 瀏覽器至 1.87.188(含)以後版本 https://community.brave.com/t/how-to-update-brave/384780 請更新 Opera 瀏覽器至 127.0.5778.64(含)以後版本 https://help.opera.com/en/latest/crashes-and-issues/#updateBrowser

- 內容說明：

  研究人員發現 Google Chrome、Microsoft Edge、Vivaldi、Brave 及 Opera 等以 Chromium 為基礎之瀏覽器存在使用釋放後記憶體(Use After Free)漏洞(CVE-2026-2441)，未經身分鑑別之遠端攻擊者可利用特製 HTML 頁面觸發記憶體錯誤，進而於瀏覽器沙箱環境執行任意程式碼。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - Google Chrome 145.0.7632.75(不含)以前版本
  - Microsoft Edge 144.0.3719.130 與 145.0.3800.58(不含)以前版本
  - Vivaldi 7.8.3925.73(不含)以前版本
  - Brave 1.87.188(不含)以前版本

- Opera 127.0.5778.64(不含)以前版本

- 資料來源：
  1. CVE-2026-2441
  2. 更新 Google Chrome
  3. Microsoft Edge 更新設定
  4. Update Vivaldi on desktop
  5. How to update brave
  6. How to update your Opera browser
  7. Stable Channel Update for Desktop
  8. Chromium: CVE-2026-2441 Use after free in CSS
  9. Minor update (2) for Vivaldi Desktop Browser 7.8
  10. Release Channel 1.87.188
  11. Opera 127.0.5778.64 Stable update

2.3.9 Cisco 旗下防火牆系統存在2個重大資安漏洞

CVE 編號	CVE-2026-20131,CVE-2026-20079
影響產品	Cisco Secure Firewall Management Center
解決辦法	依官方網站釋出的解決方式進行修補： 【CVE-2026-20131】 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh 【CVE-2026-20079】 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2

- 內容說明：

  Cisco Secure Firewall Management Center（FMC）是一套集中式管理平台，用於統一管理與監控 Cisco 防火牆產品，提供完整的威脅防禦視野，並支援政策制定、事件分析、流量監控與裝置設定等功能，近日 Cisco 發布重大資安公告。

  【CVE-2026-20131，CVSS：10.0】

  此漏洞存在於 FMC 的網頁管理介面，未經身分驗證的遠端攻擊者，可能以 root 身分執行任意 Java 程式碼。

  【CVE-2026-20079，CVSS：10.0】

  此漏洞存在於 FMC 的網頁管理介面，未經身分驗證的遠端攻擊者，可能繞過身分驗證並在受影響的裝置執行腳本，從而獲得對底層作業系統的 root 存取權限。

- 影響平台：
  - Cisco Secure Firewall Management Center (FMC) 6.4.0.13、6.4.0.14、6.4.0.15、6.4.0.16、6.4.0.17、6.4.0.18、7.0.0、7.0.0.1、7.0.1、7.0.1.1、7.0.2、7.0.2.1、7.0.3、7.0.4、7.0.5、

7.0.6 、7.0.6.1 、7.0.6.2 、7.0.6.3 、7.0.7 、7.0.8 、7.0.8.1 、7.1.0 、7.1.0.1 、7.1.0.2 、7.1.0.3 、7.2.0 、7.2.1 、7.2.2 、7.2.0.1 、7.2.3 、7.2.3.1 、7.2.4 、7.2.4.1 、7.2.5 、7.2.5.1 、7.2.6 、7.2.7 、7.2.5.2 、7.2.8 、7.2.8.1 、7.2.9 、7.2.10 、7.2.10.2 、7.2.10.1 、7.3.0 、7.3.1 、7.3.1.1 、7.3.1.2、7.4.0 、7.4.1 、7.4.1.1 、7.4.2 、7.4.2.1 、7.4.2.2 、7.4.2.3 、7.4.2.4 、7.4.3 、7.4.4 、7.4.5 、7.6.0 、7.6.1 、7.6.2 、7.6.2.1 、7.6.3 、7.6.4 、7.7.0 、7.7.10 、7.7.10.1 、7.7.11 、10.0.0 版本

- 資料來源：
  1. Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability
  2. Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
  3. CVE-2026-20131
  4. CVE-2026-20079

2.3.10 趨勢科技旗下Apex One管理控制台存在2個重大資安漏洞

CVE 編號	CVE-2025-71210,CVE-2025-71211
影響產品	Trend Micro Apex One
解決辦法	根據官方網站釋出的解決方式進行修補： https://success.trendmicro.com/en-US/solution/KA-0022458

- 內容說明：

  Apex One 是趨勢科技旗下一款端點安全整合式方案，提供集中式管理功能，可有效防護企業端點免受各種網路安全威脅侵害。日前，趨勢科技發布 2 個重大資安漏洞(CVE-2025-71210，CVSS：9.8 和 CVE-2025-71211，CVSS：9.8)，皆屬於路徑遍歷漏洞，允許未經身分認證的遠端攻擊者，可利用此漏洞上傳惡意檔案並執行任意程式碼。

- 影響平台：
  - Trend Micro Apex One 2019(On-prem)版本
- 資料來源：
  1. SECURITY BULLETIN: Apex One and Apex One (Mac) - February 2026
  2. Trend Micro Apex One Console Directory Traversal Remote Code Execution Vulnerability
  3. Trend Micro Apex One Console Directory Traversal Remote Code Execution Vulnerability

2.3.11 SAP NetWeaver 企業入口網站管理存在重大資安漏洞(CVE-2026-27685)

CVE 編號	CVE-2026-27685
影響產品	SAP NetWeaver Enterprise Portal Administration
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/march-2026.html

- 內容說明：

  SAP 針對旗下產品 SAP NetWeaver Enterprise Portal Administration 發布重大資安漏洞公告(CVE-2026-27685，CVSS：9.1)，允許具有特權的攻擊者上傳不受信任或惡意內容時，經系統反序列化處理後，可能對主機系統的機密性、完整性和可用性造成影響。

- 影響平台：
  - SAP NetWeaver Enterprise Portal Administration Version(s) - EP-RUNTIME 7.50
- 資料來源：
  1. SAP Security Patch Day - March 2026
  2. CVE-2026-27685

2.3.12 Zoom Workplace Windows版本存在重大資安漏洞(CVE-2026-30903)

CVE 編號	CVE-2026-30903
影響產品	Zoom Workplace Windows
解決辦法	根據官方網站釋出的解決方式進行修補： https://www.zoom.com/en/trust/security-bulletin/zsb-26005/

- 內容說明：

  近日 Zoom 針對 Zoom Workplace Windows 版本發布重大資安公告(CVE-2026-30903，CVSS：9.6)，該漏洞存在於郵件功能中，因檔案名稱或路徑可被外部控制，可能允許未經身分驗證的攻擊者透過網路存取系統並提升權限。

- 影響平台：
  - Zoom Workplace for Windows 6.6.0 之前的版本
  - Zoom Workplace VDI Client for Windows 版本 6.4.17、6.5.15 和 6.6.10 之前的版本
- 資料來源：
  1. Zoom Workplace for Windows - External Control of File Name or Path

2.3.13 Broadcom 旗下 Vmware 虛擬化軟體存在2個重大資安漏洞

CVE 編號	CVE-2026-22719,CVE-2026-22720
影響產品	Broadcom Vmware Aria Operations、Cloud Foundation、Telco Cloud Platform、Telco Cloud Infrastructure
解決辦法	根據官方網站釋出的解決方式進行修補： https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947

- 內容說明：

  Broadcom 針對旗下多個 Vmware 虛擬化軟體產品發布重大資安公告。

  【CVE-2026-22719，CVSS：8.1】

  此為指令注入漏洞，Aria Operations 支援協助產品遷移(support-assisted product migration)流程中，可使未經身分鑑別之遠端攻擊者利用此漏洞於受影響設備執行任意指令。

  註：目前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。

  【CVE-2026-22720，CVSS：8.0】

  此為儲存型跨網站腳本攻擊漏洞，可使具建立自訂評估標準(custom benchmark)權限之遠端攻擊者注入惡意腳本，進而以管理者權限執行系統操作。

- 影響平台：
  - VMware Aria Operations 8.05 至 8.18.6(不含)以前版本
  - VMware Cloud Foundation 4.0 至 5.2.3(不含)以前版本
  - VMware Cloud Foundation 9.0 至 9.0.2.0(不含)以前版本
  - VMware Telco Cloud Platform 4.0 至 5.1(含)以前版本
  - VMware Telco Cloud Infrastructure 2.2 至 3.0(含)以前版本

- 資料來源：
  1. VMSA-2026-0001: VMware Aria Operations updates address multiple vulnerabilities
  2. CVE-2026-22719
  3. CVE-2026-22720

2.3.14 以Chromium為基礎之瀏覽器存在10個重大資安漏洞

CVE 編號	CVE-2026-3536 至 CVE-2026-3545
影響產品	Chromium 為基礎之瀏覽器
解決辦法	請更新 Google Chrome 瀏覽器至 145.0.7632.159(含)以後版本 請更新 Microsoft Edge 瀏覽器至 145.0.3800.97(含)以後版本 請更新 Vivaldi 瀏覽器至 7.8.3925.76(含)以後版本 請更新 Brave 瀏覽器至 1.87.192(含)以後版本

- 內容說明：

  研究人員發現 Google Chrome、Microsoft Edge、Vivaldi 及 Brave 等以 Chromium 為基礎之瀏覽器存在 10 個高風險安全漏洞(CVE-2026-3536 至 CVE-2026-3545)，類型包含整數溢位(Integer Overflow)、越界寫入(Out-of-bounds Write)及沙箱逃逸(Sandbox Escape)等，攻擊者可透過特製 HTML 網頁或擴充程式存取記憶體或執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - Google Chrome 145.0.7632.159(不含)以前版本
  - Microsoft Edge 145.0.3800.97(不含)以前版本
  - Vivaldi 7.8.3925.76(不含)以前版本
  - Brave 1.87.192(不含)以前版本

- 資料來源：

1. Google Chrome 說明
2. CVE-2026-3536
3. CVE-2026-3537
4. CVE-2026-3538
5. CVE-2026-3539
6. CVE-2026-3540
7. CVE-2026-3541
8. CVE-2026-3542
9. CVE-2026-3543
10. CVE-2026-3544
11. CVE-2026-3545

2.3.15 Microsoft 旗下SharePoint Server 存在2個重大資安漏洞

CVE 編號	CVE-2026-26106,CVE-2026-26114
影響產品	Microsoft SharePoint Server
解決辦法	根據官方網站釋出的解決方式進行修補： 【CVE-2026-26106】 https://msrc.microsoft.com/update-guide/zh-tw/vulnerability/CVE-2026-26106 【CVE-2026-26114】 https://msrc.microsoft.com/update-guide/zh-tw/vulnerability/CVE-2026-26114

- 內容說明：

  Microsoft SharePoint Server 是一款企業級協作平台，提供文件管理與團隊協作等功能，是企業資訊整合的核心平台。近日 Microsoft 發布 2 個重大資安漏洞公告(CVE-2026-26106，CVSS：8.8 和 CVE-2026-26114，CVSS：8.8)。其中 CVE-2026-26106 為輸入驗證不當漏洞，允許經授權的攻擊者透過網路執行程式碼；CVE-2026-26114 為不受信任資料反序列化漏洞，允許經授權的攻擊者透過網路執行程式碼。

- 影響平台：

  【CVE-2026-26106】
  - Microsoft SharePoint Enterprise Server 2016 16.0.0 至 16.0.5543.1000 版本
  - Microsoft SharePoint Server Subion Edition 16.0.0 至 16.0.10417.20102 版本
  - Microsoft SharePoint Server 2019 16.0.0 至 16.0.19725.20076 版本

  【CVE-2026-26114】
  - Microsoft SharePoint Enterprise Server 2016 16.0.0 至 16.0.5543.1000 版本

- Microsoft SharePoint Server 2019 16.0.0 至 16.0.10417.20102 版本

- 資料來源：
  1. Microsoft SharePoint Server 遠端執行程式碼弱點
  2. Microsoft SharePoint Server 遠端執行程式碼弱點
  3. CVE-2026-26106
  4. CVE-2026-26114

2.3.16 Ivanti旗下Endpoint Manager 存在高風險資安漏洞(CVE-2026-1603)

CVE 編號	CVE-2026-1603
影響產品	Ivanti Endpoint Manager
解決辦法	根據官方網站釋出的解決方式進行修補： https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US

- 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。近期 Ivanti 發布重大資安漏洞公告(CVE-2026-1603，CVSS：8.6)，此為身分識別繞過漏洞，未經身分驗證的遠端攻擊者可取得特定身分識別資料。

  註：目前已有駭客利用此漏洞，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：
  - Ivanti Endpoint Manager 2024 SU4 SR1(含)以前版本
- 資料來源：
  1. Security Advisory EPM February 2026 for EPM 2024
  2. CVE-2026-1603

2.3.17 Cisco IOS XR Software 存在2個重大資安漏洞

CVE 編號	CVE-2026-20040,CVE-2026-20046
影響產品	Cisco IOS XR Software
解決辦法	請更新至以下版本： 【CVE-2026-20040】 Cisco IOS XR Software 25.2.21 版本 Cisco IOS XR Software 25.4.2 版本 備註：Cisco IOS XR Software 25.1(含)之前版本、25.3 版本，請遷移至固定版本 【CVE-2026-20046】 Cisco IOS XR Software 25.2.2 版本 備註：Cisco IOS XR Software 25.1(含)之前版本，請遷移至固定版本

- 內容說明：

  近日 Cisco 針對 IOS XR Software 發布重大資安公告(CVE-2026-20040，CVSS：8.8 和 CVE-2026-20046，CVSS：8.8)，皆為 CLI 權限提升漏洞。CVE-2026-20040 可能允許經過身分驗證的本機攻擊者，以 root 身分在受影響裝置的底層作業系統執行任意指令；CVE-2026-20046 存在於特定CLI指令的任務群組指派，可能允許經過身分驗證的本機攻擊者提升權限，並取得受影響裝置的完全管理控制權。

- 影響平台：

  【CVE-2026-20040】

  - Cisco IOS XR Software 25.1(含)之前版本
  - Cisco IOS XR Software 25.2 版本
  - Cisco IOS XR Software 25.3 版本

- Cisco IOS XR Software 25.4 版本

【CVE-2026-20046】

- Cisco IOS XR Software 25.1(含)之前版本
- Cisco IOS XR Software 25.2 版本

- 資料來源：
  1. Cisco IOS XR Software CLI Privilege Escalation Vulnerabilities
  2. CVE-2026-20040
  3. CVE-2026-20046

2.3.18 Veeam旗下Veeam Backup & Replication備份軟體存在多個重大資安漏洞

CVE 編號	CVE-2026-21666,CVE-2026-21667,CVE-2026-21668,CVE-2026-21672,CVE-2026-21708,CVE-2026-21669,CVE-2026-21671
影響產品	Veeam Backup & Replication
解決辦法	請更新至以下版本： Veeam Backup & Replication 12.3.2.4465 版本 Veeam Backup & Replication 13.0.1.2067 版本

- 內容說明：

  Veeam Backup & Replication 是 Veeam 核心備份軟體，近日 Veeam 發布重大資安漏洞公告。

  【CVE-2026-21666，CVSS：9.9】

  允許經過驗證的網域使用者在備份伺服器上遠端執行程式碼。

  【CVE-2026-21667，CVSS：9.9】

  允許經過驗證的網域使用者在備份伺服器上遠端執行程式碼。

  【CVE-2026-21668，CVSS：8.8】

  允許經過身分驗證的網域使用者繞過限制，並操縱備份儲存庫中的任意檔案。

  【CVE-2026-21672，CVSS：8.8】

  基於 Windows 的 Veeam Backup & Replication 伺服器，存在本機權限提升漏洞。

  【CVE-2026-21708，CVSS：9.9】

  允許備份檢視器以使用者身分遠端執行程式碼。

  【CVE-2026-21669，CVSS：9.9】

  允許經過驗證的網域使用者在備份伺服器上遠端執行程式碼。

  【CVE-2026-21671，CVSS：9.1】

允許具有備份管理員角色的已認證使用者在 Veeam Backup & Replication 的高可用性 (HA) 部署中遠端執行程式碼。

- 影響平台：

  【CVE-2026-21666、CVE-2026-21667、CVE-2026-21668、CVE-2026-21672、CVE-2026-21708】

  - Veeam Backup & Replication 12.3.2.4165 (含)之前版本

  【CVE-2026-21669、CVE-2026-21671、CVE-2026-21672、CVE-2026-21708】

  - Veeam Backup & Replication 13.0.1.1071 (含)之前版本
- 資料來源：
  1. Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2.4465
  2. Vulnerabilities Resolved in Veeam Backup & Replication 13.0.1.2067
  3. CVE-2026-21666
  4. CVE-2026-21667
  5. CVE-2026-21668
  6. CVE-2026-21672
  7. CVE-2026-21708
  8. CVE-2026-21669
  9. CVE-2026-21671

2.3.19 HPE Aruba Networking AOS-CX 存在2個重大資安漏洞

CVE 編號	CVE-2026-23813,CVE-2026-23814
影響產品	Aruba Networking AOS-CX
解決辦法	根據官方網站釋出的解決方式進行修補： https://networkingsupport.hpe.com/home/

- 內容說明：

  近期 HPE 針對 Aruba Networking AOS-CX 發布重大資安公告(CVE-2026-23813，CVSS：9.8 和 CVE-2026-23814，CVSS：8.8)。CVE-2026-23813 存在於 AOS-CX 交換器的 Web 的管理介面，可能允許未經身分驗證的遠端攻擊者繞過身分驗證機制，在某些情況下，可能導致管理員密碼重設；CVE-2026-23814 為命令注入漏洞，可能允許經過身分驗證且具有低權限的遠端攻擊者，注入和執行惡意命令。

- 影響平台：
  - AOS-CX 10.17.0001 (含)以下版本
  - AOS-CX 10.16.1020 (含)以下版本
  - AOS-CX 10.13.1160 (含)以下版本
  - AOS-CX 10.10.1170 (含)以下版本
- 資料來源：
  1. HPESBNW05027 rev.1 - HPE Aruba Networking AOS-CX, Multiple Vulnerabilities
  2. CVE-2026-23813
  3. CVE-2026-23814

2.3.20 Oracle Identity Manager 和 Oracle Web Services Manager 存在重大資安漏洞(CVE-2026-21992)

CVE 編號	CVE-2026-21992
影響產品	Oracle Identity Manager、Web Services Manager
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/-cve-2026-21992.html

- 內容說明：

  近日 Oracle 針對 Identity Manager (元件: REST WebServices)和 Web Services Manager(元件: Web Services Security)發布重大資安公告(CVE-2026-21992，CVSS：9.8)，該漏洞允許未經身分驗證的遠端攻擊者可遠端程式碼執行。

- 影響平台：
  - Oracle Identity Manager 12.2.1.4.0 版本
  - Oracle Identity Manager 14.1.2.1.0 版本
  - Oracle Web Services Manager 12.2.1.4.0 版本
  - Oracle Web Services Manager 14.1.2.1.0 版本
- 資料來源：
  1. Oracle Security Alert Advisory - CVE-2026-21992
  2. CVE-2026-21992

2.3.21 Citrix旗下NetScaler ADC 和 NetScaler Gateway 存在重大資安漏洞(CVE-2026-3055)

CVE 編號	CVE-2026-3055
影響產品	NetScaler ADC、NetScaler Gateway
解決辦法	請更新至以下版本： NetScaler ADC 和 NetScaler Gateway 14.1-60.58(含)之後版本 NetScaler ADC 和 NetScaler Gateway 13.1-62.23(含)之後版本 NetScaler ADC FIPS and NDcPP 13.1-37.262(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-2026-3055，CVSS 4.x：9.3)，此為越界讀取漏洞，起因為輸入驗證不足導致記憶體過度讀取。

- 影響平台：
  - NetScaler ADC 和 NetScaler Gateway 14.1-60.58(不含)之前版本
  - NetScaler ADC 和 NetScaler Gateway 13.1-62.23(不含)之前版本
  - NetScaler ADC FIPS and NDcPP 13.1-37.262(不含)之前版本
- 資料來源：
  1. NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2026-3055 and CVE-2026-4368
  2. CVE-2026-3055

2.3.22 QNAP作業系統存在高風險資安漏洞(CVE-2025-66277)

CVE 編號	CVE-2025-66277
影響產品	QNAP QTS、QuTS hero
解決辦法	根據官方網站釋出的解決方式進行修補： https://www.qnap.com/en/security-advisory/qsa-26-05

- 內容說明：

  研究人員發現 QNAP 作業系統存在連結追蹤(Link Following)漏洞(CVE-2025-66277，CVSS 3.x：9.8)，未經身分鑑別之遠端攻擊者可利用此漏洞存取未授權之檔案系統路徑，請儘速確認並進行修補。

- 影響平台：
  - QTS 5.2.x 至 5.2.8.3350 build 20251216(不含)版本
  - QuTS hero h5.2.x 至 h5.2.8.3350 build 20251216(不含)版本
- 資料來源：
  1. Multiple Vulnerabilities in QTS and QuTS hero
  2. CVE-2025-66277

第 3 章、資安研討會及活動

- **資安研討會**

【研討會】115/4/16 AI賦能資安防護：構築永不疲倦資安韌性防禦	
活動時間	2026-04-16 13:30 ~ 2026-04-16 17:00
活動地點	臺大醫院國際會議中心402AB會議室(臺北市中正區徐州路2號)
活動網站	https://www.tissa.org.tw/Course/Detail/5967
活動概要	 **【費用】** 免費，全程參與本次研討會有3小時「公務人員學習時數」，或提供電子時數證明文件 報名截止： 2026-04-14 **【活動內容 / Event Deails】** 面對 AI 浪潮，您的資安跟上了嗎？在風險無所不在的數位時代，需要的不只是防守，而是提前預警、即時阻擋、快速回應的全方位守護。本活動聚焦「以 AI 強化防禦」，匯集專家深入解析，以自動化機制主動揪出隱藏漏洞，守住營運、穩住信任。 現場亦有奧義智慧、眾至資訊、智慧資安、騰曜網路科技、偉康科技、勤晁科技 等

	多家展示解決方案，帶來最新技術與實務分享！用 AI 對抗 AI，立刻跟上～ **【主辦單位】中華民國資訊軟體服務商業同業公會、資安韌性促進會** **【聯絡窗口】02-2553-3988#812 盧資深專員** **security@tissa.org.tw**

CYBERSEC 2026 臺灣資安大會	
活動時間	**2026-05-05 ~ 2026-05-07**
活動地點	**南港展覽館 2 館**
活動網站	**https://r.itho.me/CYBERSEC_TWCERTCC**
活動概要	 **【費用】** 免費線上報名【現場報名將收取作業費 500 元】 **【活動內容 / Event Deails】** CYBERSEC 2026 臺灣資安大會以「RESILIENT FUTURE」為年度主題，深刻回應風險常態化的時代挑戰。安全的定義持續演變，防禦的核心不再只是阻擋風險，更是承受衝擊、迅速恢復，並維持運作的韌性；在每一次試煉中，實現越戰越強的自我進化。大會攜手

	全球資安專家與技術團隊，規劃超過 300 場專業演說，並集結 400 多家國際資安品牌參與展出，預計將吸引兩萬名資安專業人士共襄盛舉，鏈結全球資安技術能量。 **亞洲最具指標資安會展與交流平台，規模再創新高：** ● 萬人盛會｜20,000+ 專業人士共襄盛舉，深化產業技術交流 ● 企業首選｜4,000+ 企業指定觀展，掌握產業實務應用 ● 技術殿堂｜300+ 場專業議程，匯聚全球防禦實戰經驗 ● 國際規格｜3 日會期、30 國參與，臺灣唯一的國際級資安盛事

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：

全景軟體｜IDExpert Windows Logon Agent - 存在2個漏洞	
TVN / CVE ID	TVN-202603001 / CVE-2026-2999, CVE-2026-3000
CVSS	CVE-2026-2999： 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVE-2026-3000： 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	IDExpert Windows Logon Agent 2.7.3.230719至2.8.4.250925版本
問題描述	CVE-2026-2999(Remote Code Execution)： 未經身分鑑別之遠端攻擊者可使系統下載遠端任意執行檔案並執行。 CVE-2026-3000(Remote Code Execution)： 未經身分鑑別之遠端攻擊者可使系統下載遠端任意DLL檔案並執行。
解決方法	聯繫廠商進行修補，或至全景官網下載修補工具。 官網連結： https://www.changingtec.com/news_detail.jsp?item_id=348
公開日期	2026-03-02
相關連結	**https://www.twcert.org.tw/tw/cp-132-10740-b2eb2-1.html**
一等一科技｜U-Office Force - Insecure Deserialization	

TVN / CVE ID	TVN-202603002 / CVE-2026-3422
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	U-Office Force 29.50(含)以前版本
問題描述	一等一科技開發之U-Office Force存在Insecure Deserialization漏洞，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	請更新至29.50SP1(含)之後版本
公開日期	2026-03-02
相關連結	https://www.twcert.org.tw/tw/cp-132-10742-45b13-1.html
上尚科技｜EHG2408系列交換器 - Stack-based Buffer Overflow	
TVN / CVE ID	TVN-202603004 / CVE-2026-3823
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	EHG2408/EHG2408-2SFP韌體v3.36(不含)以前版本
問題描述	上尚科技開發之EHG2408系列交換器存在Stack-based Buffer Overflow漏洞，未經身分鑑別之遠端攻擊者可控制程式執行流程進而執行任意程式碼。
解決方法	請更新韌體至v3.36(含)以後版本
公開日期	2026-03-09
相關連結	https://www.twcert.org.tw/tw/cp-132-10752-5a4d9-1.html
葳橋資訊｜單一簽入暨電子目錄服務系統 - Local File Inclusion	
TVN / CVE ID	TVN-202603005 / CVE-2026-3826
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	單一簽入暨電子目錄服務系統 IFTOP_P4_181(不含)以前版本

問題描述	CVE-2026-3826(Local File Inclusion)： 未經身分鑑別之遠端攻擊者可利用此漏洞於伺服器端執行任意程式碼。
解決方法	更新至IFTOP_P4_181(含)以後版本
公開日期	2026-03-11
相關連結	https://www.twcert.org.tw/tw/cp-132-10755-94136-1.html
中華龍網｜GCB/FCB政府金融資安組態稽核軟體 - Missing Authentication	
TVN / CVE ID	TVN-202603006 / CVE-2026-4312
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	GCB/FCB政府金融資安組態稽核軟體20260108(不含)以前版本
問題描述	中華龍網開發之GCB/FCB政府金融資安組態稽核軟體存在Missing Authentication漏洞，未經身分鑑別之遠端攻擊者可直接使用API功能新增管理權限帳號。
解決方法	更新至20260108(含)以後版本
公開日期	2026-03-17
相關連結	https://www.twcert.org.tw/tw/cp-132-10784-4f67d-1.html
叡揚資訊｜Vitals ESP - Incorrect Authorization	
TVN / CVE ID	TVN-202603007 / CVE-2026-4639
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	Vitals ESP 6.3(含)以前版本
問題描述	CVE-2026-4639(Incorrect Authorization)： 已通過身分鑑別之遠端攻擊者可執行部分管理權限功能，進而提升權限。

解決方法	聯繫廠商進行修補
公開日期	2026-03-23
相關連結	**https://www.twcert.org.tw/tw/cp-132-10794-704a2-1.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3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/**