TWCERT/CC 資安情資電子報

2026 年 10 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

目錄 II

第 1 章、封面故事 1

Node.js發布安全性更新修補10項漏洞，其中CVE-2026-111497可導致遠端程式碼執行，籲儘速更新 1

第 2 章、國內外重要資安事件 5

2.1 新興應用資安 5

2.1.1 駭客利用AI滲透測試工具ARTEX竊取韓國金融業資料 5

2.2 軟硬體系統資安議題 9

2.2.1 PHP發布安全性更新修補2項可導致遠端程式碼執行之嚴重漏洞，國際資安機構籲儘速更新 9

2.3 軟硬體漏洞資訊 14

2.3.1 NetScaler ADC與NetScaler Gateway存在3個重大資安漏洞 14

2.3.2 Cisco ISE與ISE-PIC存在5個高風險安全漏洞 16

2.3.3 Cisco Secure FMC存在2個高風險安全漏洞 18

2.3.4 Zyxel GS1900系列交換器存在高風險安全漏洞(CVE-2026-7273) 19

2.3.5 Cisco Catalyst SD-WAN 存在重大資安漏洞(CVE-2026-76504) 20

2.3.6 Microsoft Office SharePoint存在高風險安全漏洞(CVE-2026-65660) 22

2.3.7 pgAdmin 4存在高風險安全漏洞(CVE-2026-86863) 23

2.3.8 Check Point多項產品存在高風險安全漏洞(CVE-2026-93616) 24

2.3.9 F5 BIG-IP APM存在高風險安全漏洞(CVE-2026-94127) 25
2.3.10 SonicWall 旗下SMA1000系列產品存在重大資安漏洞 (CVE-2026-102255) 26
2.3.11 Veeam旗下Veeam Backup & Replication備份軟體存在重大資安漏洞(CVE-2025-64393) 27
2.3.12 Cisco 旗下 Nexus 3000 和 9000系列交換器存在4個重大資安漏洞 28
2.3.13 Splunk Enterprise存在高風險安全漏洞(CVE-2026-76268)，請儘速確認並進行處置 ... 29
2.3.14 Ivanti Neurons for Intune 存在重大資安漏洞(CVE-2026-109412) 30
2.3.15 Ivanti旗下Xtraction存在高風險資安漏洞(CVE-2026-106042) 31
2.3.16 FortiSIEM 存在重大資安漏洞(CVE-2026-106173) 32
2.3.17 FortiSandbox GUI 存在重大資安漏洞(CVE-2026-107656) 33
2.3.18 FortiAnalyzer、FortiManager、FortiManager Cloud 和 FortiAnalyzer Cloud 存在重大資安漏洞(CVE-2025-46773) 34
2.3.19 Cisco License (Smart Software Manager) On-Prem 存在2個重大資安漏洞 36
2.3.20 Cisco NX-OS Software NX-API 存在重大資安漏洞(CVE-2026-76471) 37
2.3.21 SonicWall NSM On-Prem 存在重大資安漏洞(CVE-2026-96540) 38
2.3.22 Cisco Secure Email Gateway 存在重大資安漏洞(CVE-2026-76519) 39
2.3.23 Cisco License (Smart Software Manager) On-Prem 存在4個重大資安漏洞 40
2.3.24 Cisco NX-OS Software NX-API 存在3個重大資安漏洞 41
2.3.25 Cisco Application Policy Infrastructure Controller 存在3個重大資安漏洞 44
2.3.26 Cisco Meraki 存在 4 個重大資安漏洞 45
2.3.27 Dell System Update存在高風險安全漏洞(CVE-2026-86360)，請儘速確認並進行處置 48
2.3.28 GitLab AI Gateway存在高風險安全漏洞(CVE-2026-90970)，請儘速確認並進行處置 .. 49
2.3.29 PHP 存在2個重大資安漏洞(CVE-2026-109618 和 CVE-2026-109619) 50

2.3.30 Node.js 存在4個重大資安漏洞，請儘速確認並進行處置 52
2.3.31 GitLab存在2項高風險安全漏洞(CVE-2026-97229與CVE-2026-110264) 54
2.3.32 Oracle Java SE與Oracle GraalVM存在高風險安全漏洞(CVE-2026-91403)，請儘速確認並進行處置 56
2.3.33 Go存在高風險安全漏洞(CVE-2026-111943)，請儘速確認並進行處置 57
2.3.34 Fortinet 多款資安產品釋出安全強化更新，請儘速確認並完成更新 58
第 3 章、資安研討會及活動 60
第 4 章、TVN 漏洞公告 63
編輯：TWCERT/CC 團隊 69

第 1 章、封面故事

Node.js發布安全性更新修補10項漏洞，其中CVE-2026-111497可導致遠端程式碼執行，籲儘速更新

Node.js官方於2026年10月21日發布安全性更新，針對22.x、24.x及26.x版本線共修補10項漏洞，其中4項為高風險，包含可導致遠端程式碼執行之Brotli解碼器越界寫入漏洞（CVE-2026-111497）。數位發展部資通安全署亦於10月22日發布新聞稿，呼籲各機關與企業儘速完成更新。Node.js常見於後端服務、容器映像檔、網頁前端工具鏈及部分AI agent

命令列工具中，建議企業盤點環境中之Node.js版本並儘速更新。

Node.js官方公告

Node.js官方於2026年10月21日發布22.23.4、24.22.1及26.12.1版本，共修補10項漏洞，包含高風險4項、中風險3項及低風險3項。其中高風險漏洞如下：

CVE編號	漏洞說明	影響版本線
CVE-2026-111497	Brotli解碼器存在越界寫入（Out-of-Bounds Write）缺陷，可導致遠端程式碼執行	22.x、24.x、26.x
CVE-2026-105482	dns.resolve函式處理含NUL字元之名稱時，會將名稱截斷	22.x、24.x、26.x
CVE-2026-105483	IP位址以全形數字書寫時，可繞過TLS憑證之主機名稱檢查	24.x、26.x
CVE-2026-106069	主機名稱可被寬鬆解析為IP位址時，可繞過TLS憑證之主機名稱檢查	22.x、24.x、26.x

表1、Node.js 2026年10月安全性更新之高風險漏洞（資料來源：Node.js官方公告）

其餘6項中、低風險漏洞涉及連線處理、隨機數重複產生及權限模型（Permission Model）繞過等問題。本次更新亦同步更新Node.js內建之憑證清單，以因應印度憑證機構eMudhra中繼憑證遭入侵事件。官方另指出，已停止支援（End-of-Life）之版本一律受影響，且不會提供修補。

版本線	受影響版本	修補版本
Node.js 22.x	22.23.4之前版本	22.23.4
Node.js 24.x	24.22.1之前版本	24.22.1
Node.js 26.x	26.12.1之前版本	26.12.1
Node.js 20.x及更早版本線	已停止支援	升級至受支援版本線

表2、Node.js受影響版本與修補版本（資料來源：Node.js官方公告）

企業常見使用情境：

Node.js應用範圍廣泛，以下為常見之使用情境，建議一併納入盤點範圍：

- 後端服務：微服務架構及各類API伺服器。
- 容器映像檔：伺服器主機及容器化映像檔（Docker Images）中之Node.js版本均需檢視並完成升級。
- 網頁前端工具鏈：網頁前端開發所使用之工具鏈。
- 透過npm安裝之命令列工具：部分AI agent命令列工具（如Gemini CLI）以Node.js為執行環境，使用者電腦上之Node.js版本亦需一併更新。

建議措施：

- 盤點環境中使用Node.js之系統，包含伺服器主機、容器映像檔及使用者電腦，可於終端機執行「node -v」確認版本，或以軟體物料清單（SBOM）協助篩選。依美國網路安全暨基礎設施安全局（CISA）說明，由原始碼產生之SBOM依語言或生態系不同，可能未包含執行環境元件，盤點時應確認是否涵蓋Node.js本身之版本。
- 儘速更新至22.23.4、24.22.1或26.12.1以上版本，更新後重新啟動相關服務及工具；容器映像檔亦應一併完成升級。
- 使用Node.js 20.x或更早版本線者，應升級至仍受支援之版本線。

- 相關連結
  1. Node.js — Wednesday, October 21, 2026 Security Releases
  2. 資通安全署 Node.js與Go釋出緊急安全更新 資安署籲請公私部門加速修補防範遠端執行與憑證攔截風險
  3. Gemini CLI Installation
  4. CISA Types of Software Bill of Materials (SBOM)

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 駭客利用AI滲透測試工具ARTEX竊取韓國金融業資料

資安廠商CrowdStrike於2026年10月7日揭露一起涉及韓國金融機構的資料竊取事件，指出攻擊者疑似濫用名為ARTEX的AI輔助滲透測試工具發動攻擊。研究人員從攻擊者的公開目錄，取得ARTEX的相關設定檔與操作紀錄。發現攻擊活動涉及多種大型語言模型及代理伺服器(Proxy)，顯示攻擊者可能運用 AI 工具輔助執行攻擊作業。顯示攻擊者可能運用 AI 工具輔助執行攻擊作業。目前尚未將相關活動歸因至特定進階持續性威脅（Advanced Persistent Threat, APT）組織。

另外，依據韓國金融委員會於2026年10月16日公布的調查報告，當地共有16家金融企業發生資料外洩事件，總計涉及約10萬筆客戶資料。然而，前述事件是否皆與ARTEX攻擊活動相關，目前仍待進一步釐清。

ARTEX原為滲透測試(Penetration Testing)工具，可透過大型語言模型處理測試指令，協助執行入侵模擬及系統弱點檢測。根據CrowdStrike 分析，2026年9月下旬至10月上旬的相關紀錄，包含AI工具Claude Code對話與記憶檔操作日誌。攻擊者主要採用DeepSeek v4.1-flash，攻擊者另在Claude Code工作階段使用GLM-5.3與Grok 4.6，顯示其可能透過不同 AI 模型協助執行攻擊作業。

此外，攻擊者以雲端主機作為操作環境相關行為可對應 MITRE ATT&CK 技術編號 T1583.003(Virtual Private Server) 及T1588.007(Artificial Intelligence)。同時，攻擊者亦透過代理伺服器轉送網路流量，以增加追查來源的難度。

CrowdStrike 公布9個相關代理IP位址，建議企業回溯內部日誌時，將其納入威脅情資比對，並交叉檢視防火牆、VPN、代理伺服器及其他網路設備的連線紀錄，以及資料庫查詢與資料傳輸紀錄，以確認是否存在異常存取或資料外傳行為。

根據韓國金融委員會於2026年10月14日公布的外洩統計調查，受影響資料包含客戶姓名、聯絡資訊、電子郵件及韓國住民登錄號（相當於臺灣的身分證字號），暫無帳戶密碼或信用卡號外洩通報。主管機關亦要求業者封鎖攻擊來源、修補現存弱點，並於必要時暫停對外服務以策安全。

此外，研究人員根據攻擊者操作紀錄研判，攻擊者可能使用中文，但目前尚無足夠證據將其歸因至特定威脅組織。至於攻擊者如何取得初

始存取權限、是否利用特定軟體弱點，以及相關受影響軟體版本、CVE編號與 CVSS 嚴重度評分，現有公開資訊尚未提供明確說明。而ARTEX開發者Autumn-27雖已於2026年10月8日宣布停止更新與維護，並關閉公開原始碼，然而，工具停止維護並不代表既有攻擊活動或相關威脅已獲控制，企業仍應持續追蹤後續調查與威脅情資。

為防範類似利用AI自動化工具進行之資料探測與滲透攻擊，TWCERT/CC建議企業與組織採取以下防護措施：

1. 清查所有對外服務：盤點所有客戶查詢、員工內部使用及委外廠商連線的網站與API，確認系統維運負責人，關閉未使用的管理介面與不必要之外部入口，並儘速修補已知弱點。
2. 強化資料查詢權限與存取控制：針對涉及個人資料之查詢功能進行權限邊界測試，包含以未登入與低權限身分測試，落實伺服器端對每次請求的身分與權限檢查，嚴防越權存取漏洞。
3. 比對威脅指標（IoC）與異常行為：依表1所列之入侵指標，交叉檢視防火牆、VPN、代理伺服器及資料庫日誌，重點清查大量或異常的資料庫查詢與對外連線。若確認遭受滲透，應立即將受害主機隔離離線，並遵循數位鑑識程序完整保存日誌證據。
4. 落實事件通報與後續風險管控：若確認資料外洩或受影響客戶，應即刻盤點受影響個資範疇與受害用戶，並依適用規定通報並告知當事人，同時強化多因子驗證(MFA)，以降低後續衍生風險。

彙整相關威脅指標如下，建議企業/組織回朔期程至少涵蓋2026年9月下旬至10月上旬：

類型	IoC	說明
IP	38.244.50[.]120	部署ARTEX主機
IP	101.53.80[.]20	Proxy IP
IP	205.214.59[.]31	Proxy IP
IP	124.155.252[.]63	Proxy IP
IP	154.201.79[.]246	Proxy IP
IP	23.248.249[.]90	Proxy IP
IP	23.158.220[.]98	Proxy IP
IP	103.248.148[.]84	Proxy IP
IP	203.160.133[.]172	Proxy IP
IP	209.209.85[.]38	Proxy IP

表1：ARTEX攻擊事件相關入侵指標。資料來源：CrowdStrike

- 相關連結
  1. Authorities Hold Meeting on Cybersecurity Management in Financial Sector to Bolster Anti-Hacking
  2. ARTEX 安全聲明（Autumn-27）
  3. Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance

2.2 軟硬體系統資安議題

2.2.1 PHP發布安全性更新修補2項可導致遠端程式碼執行之嚴重漏洞，國際資安機構籲儘速更新

PHP官方於2026年10月21日發布安全性更新，修補CVE-2026-109618及CVE-2026-109619兩項嚴重漏洞，CVSS v4.0基礎分數皆為9.2，未經身分驗證之攻擊者可能利用漏洞執行遠端程式碼。TWCERT/CC已發布漏洞警訊公告，美國網路安全暨基礎設施安全局（CISA）、歐盟電腦緊急應變小組（CERT-EU）及英國國家網路安全中心（NCSC）等機構相繼發布警告，呼籲使用PHP之單位立即完成更新；若無法立即更新，應考慮隔離對外系統或暫停服務。

PHP官方公告

PHP官方於2026年10月20日預告，將於10月21日14:00 UTC（台灣時間22:00）發布安全性更新，修補2項嚴重漏洞，並表示若漏洞細節提前公開或出現實際利用跡象，將提前發布。

PHP官方於10月21日發布更新，修補之漏洞如下：

CVE編號	漏洞類型	CVSS v4.0 基礎分數
CVE-2026-109618	遠端程式碼執行	9.2
CVE-2026-109619	遠端程式碼執行	9.2

表1、PHP於2026年10月21日修補之漏洞（資料來源：PHP安全公告）

依官方說明，CVE-2026-109618與記憶體不足之處理機制有關，可能使PHP在請求資料尚未完成初始化時中斷，後續清理程序誤將無效資料視為有效資料。CVE-2026-109619則是請求所屬之內部狀態於記憶體釋放後仍殘留，同一處理程序後續處理之請求可能在初始化前使用該狀態。

受影響範圍涵蓋所有處理網頁請求之PHP環境，包括PHP-FPM、Apache mod_php、php-cgi、FrankenPHP及LiteSpeed。官方認為Apache mod_php風險最高，並已驗證未經身分驗證之請求可於應用程式碼執行前觸發攻擊。

各版本之修補方式如下：

版本	修補方式
PHP 8.5	更新至8.5.12
PHP 8.4	更新至8.4.27
PHP 8.3	更新至8.3.36
PHP 8.2	更新至8.2.35（2026年12月31日結束生命週期）
PHP 8.1及更早版本	不再接收官方更新，應洽詢發行版或長期支援廠商，或升級至受

	支援版本；官方另為7.4、8.0、8.1提供精簡原始碼修補

表2、PHP各版本修補方式（資料來源：PHP安全公告）

官方強調，更新為唯一完整之解決方式。公告中雖列出可降低特定攻擊路徑曝險之暫時設定，但該等措施無法確保系統安全。

國際資安機構示警

CISA呼籲各組織立即修補兩項漏洞，並更新至官方修補版本。

CERT-EU於安全公告中指出，漏洞技術細節已公開討論，初步概念驗證（PoC）開始流傳，攻擊者已利用漏洞之可能性因此升高，建議立即修補；無法立即修補者，應考慮將對外應用程式與公共網路隔離，直至修補完成並經驗證。CERT-EU並提醒，許多商用及開源產品以PHP作為後端技術，即使未直接對外提供PHP服務亦可能受影響，可參考荷蘭國家網路安全中心（NCSC-NL）彙整之受影響產品清單。

英國NCSC表示，使用任何版本PHP之組織均受影響，建議全面盤點基礎設施中執行PHP之系統並優先處理對外系統，同時留意內嵌PHP之設備與服務供應商更新；無法更新或套用暫時措施時，應考慮將系統下線，並檢查是否有遭入侵或植入後門之跡象。

日本情報處理推進機構（IPA）於修補發布前發布事前準備呼籲，並表示目前未確認有利用該漏洞之攻擊。日本國家網路安全統括室亦於X發文，呼籲儘速套用更新，並指出若難以迅速完成修補，暫時停止網站運作亦為降低風險之有效方式之一。

另依路透社報導，芬蘭國家資訊科技中心Valtori於修補發布前預防性關閉政府對外網路服務，並表示未發現漏洞遭利用之嘗試。荷蘭國會二院、NCSC等機關網站亦預防性暫停服務。

建議措施

TWCERT/CC提醒，網站由委外廠商建置或代管業者維運之單位，應主動向廠商確認PHP版本及修補狀態，使用WordPress、Drupal、Joomla、Magento等以PHP運作之內容管理系統者，亦應一併確認；另因初步PoC已開始流傳，已完成更新之系統亦宜檢視存取紀錄，確認修補前是否已有遭入侵跡象。TWCERT/CC建議採取下列措施：

- 儘速更新至PHP 8.5.12、8.4.27、8.3.36或8.2.35；使用Linux發行版套件或長期支援服務者，應向供應商確認已提供更新套件。
- 使用PHP 8.1及更早版本者，應洽詢供應商是否提供修補，或升級至受支援版本。
- 全面盤點使用PHP之系統並優先處理對外服務，範圍應涵蓋內嵌PHP之設備、第三方軟體及服務，並持續留意相關供應商發布之更新。
- 若無法立即完成更新，應考慮將對外系統與網際網路隔離或暫停服務。
- 無法立即更新或停用之系統，應於完成更新或緩解前檢查是否有遭入侵跡象，並清查是否遭植入後門。
- 使用PHP 8.2者，應於2026年12月31日結束生命週期前規劃升級。

- 相關連結

1. PHP 存在2個重大資安漏洞(CVE-2026-109618 和 CVE-2026-109619)（2026/10/22）
2. PHP Security advisory: Critical remote code execution vulnerabilities, update now（2026/10/21）
3. PHP 8.2.35 Released（2026/10/21）

4. PHP Upcoming Critical PHP Security Release（2026/10/20）
5. CVE-2026-109618
6. CVE-2026-109619
7. CISA Critical Vulnerabilities in PHP Require Immediate Patching（2026/10/21）
8. CERT-EU Security Advisory 2026-018: Critical Vulnerabilities in PHP（2026/10/21）
9. NCSC UK Critical security issue affecting PHP（2026/10/21）vulnerabilities
10. NCSC-NL php2shell受影響產品清單
11. IPA【事前準備のお願い】PHPのセキュリティリリース公開予定について（2026/10/21）
12. 國家網路安全統括室X貼文：暫時停止網站等措施（2026/10/21）
13. 國家網路安全統括室X貼文：PHP更新程式已發布（2026/10/21）
14. Reuters: Websites taken offline over PHP risks（2026/10/21）
15. NOS: Steeds meer websites offline gehaald vanwege lek, risico op hacks（2026/10/21）

2.3 軟硬體漏洞資訊

2.3.1 NetScaler ADC與NetScaler Gateway存在3個重大資安漏洞

CVE 編號	CVE-2026-88771,CVE-2026-88772,CVE-2026-88773
影響產品	NetScaler ADC 與 NetScaler Gateway
解決辦法	請更新至以下版本： NetScaler ADC 和 NetScaler Gateway 14.1-73.37 (含)之後版本、 NetScaler ADC 和 NetScaler Gateway 13.1-64.23 (含)之後版本、 NetScaler ADC FIPS 14.1-73.37(含)之後版本、 NetScaler ADC FIPS 與 NDcPP 13.1-37.279(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-2026-88771，CVSS 4.x：9.5、CVE-2026-88772，CVSS 4.x：9.5、CVE-2026-88773，CVSS 4.x：9.3)。

  其中，CVE-2026-88771 和 CVE-2026-88772 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-2026-88772，此為記憶體溢位漏洞，可導致遠端任意程式碼執行(RCE)或阻斷服務(DoS)。

  CVE-2026-88773，此漏洞為 HTTP 請求解析不一致。

CVE-2026-88771，此為輸入驗證不當漏洞，可允許未經身分驗證的攻擊者遠端執行任意程式碼(RCE)。

- 影響平台：
  - NetScaler ADC 與 NetScaler Gateway 14.1-73.37(不含)以前版本
  - NetScaler ADC 與 NetScaler Gateway 13.1-64.23(不含)以前版本
  - NetScaler ADC FIPS 14.1-73.37(不含)以前版本
  - NetScaler ADC FIPS 與 NDcPP 13.1-37.279(不含)以前版本
- 資料來源：
  1. Citrix NetScaler ADC and Citrix NetScaler Gateway Security Bulletin
  2. CVE-2026-88773
  3. CVE-2026-88772
  4. CVE-2026-88771

2.3.2 Cisco ISE與ISE-PIC存在5個高風險安全漏洞

CVE 編號	CVE-2026-20130,CVE-2026-20192,CVE-2026-20307,CVE-2026-76423,CVE-2026-76460
影響產品	Cisco ISE 與 ISE-PIC
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：

  研究人員發現 Cisco ISE 與 ISE-PIC 存在多項高風險安全漏洞(CVE-2026-20130，CVSS:10.0、CVE-2026-20192，CVSS:10.0、CVE-2026-20307，CVSS:9.9、CVE-2026-76423，CVSS:10.0 及 CVE-2026-76460，CVSS:10.0)。其中 CVE-2026-76460 已遭駭客濫用，請儘速確認並進行修補。

  CVE-2026-76460，未經身分鑑別之遠端攻擊者可藉由向存在缺陷之 API 端點傳送特製請求，繞過網頁管理介面之身分鑑別，進而未授權存取受影響裝置。

  CVE-2026-76423，未經身分鑑別之遠端攻擊者可藉由向對外開放之 REST API 連接埠傳送特製 HTTP 請求，以管理者權限讀取及變更 ISE 組態與身分資料。

  CVE-2026-20307，已通過身分鑑別之遠端攻擊者可藉由向網頁管理介面傳送特製之 Java 序列化物件，於底層作業系統執行任意程式碼，並將權限提升至 root。

  CVE-2026-20192，未經身分鑑別之遠端攻擊者可繞過身分鑑別與授權限制，進而未授權存取受影響裝置。

  CVE-2026-20130，未經身分鑑別之遠端攻擊者可藉由在傳遞至下游元件之輸出中，植入未經妥善處理之特殊元素，於受影響裝置執行任意程式碼。

- 影響平台：
  - Cisco ISE 與 ISE-PIC 3.1 至 3.5 版本、
  - Cisco ISE 與 ISE-PIC 3.0(含)以前版本(已終止軟體維護)
- 資料來源：
  1. Cisco Identity Services Engine Authentication Bypass Vulnerability
  2. Cisco Identity Services Engine Vulnerabilities
  3. Cisco Identity Services Engine Remote Code Execution Vulnerabilities
  4. Cisco Identity Services Engine Hardening Release: September 2026
  5. CVE-2026-20130
  6. CVE-2026-20192
  7. CVE-2026-20307
  8. CVE-2026-76423
  9. CVE-2026-76460

2.3.3 Cisco Secure FMC存在2個高風險安全漏洞

CVE 編號	CVE-2026-20242,CVE-2026-20324
影響產品	Cisco Secure FMC
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：

  研究人員發現 Cisco Secure FMC 存在多項高風險安全漏洞(CVE-2026-20242，CVSS:9.8 與 CVE-2026-20324，CVSS:9.9)。

  CVE-2026-20324，當啟用 sftunnel 通訊協定時(系統預設為啟用)，已通過身分鑑別之遠端攻擊者可藉由劫持 sftunnel 連線，或冒用合法註冊之 sftunnel 對端身分傳送指令，將惡意檔案寫入裝置任意位置，並以 root 權限執行任意程式碼。

  CVE-2026-20242，當啟用外部資料庫存取(External Database Access)功能，且存取清單中已設定主機時，未經身分鑑別之遠端攻擊者可從清單內之主機向特定 TCP 連接埠傳送特製之 Java 序列化位元組串流，進而於受影響裝置以 root 權限執行任意指令。

- 影響平台：
  - Cisco Secure FMC 7.0.0 至 7.0.9、7.2.0 至 7.2.11、7.3.0 至 7.3.1.2、7.4.0 至 7.4.7、7.6.0 至 7.6.5、7.7.0 至 7.7.12 及 10.0.0 至 10.0.1 版本
- 資料來源：
  1. Cisco Secure Firewall Management Center Software Java Deserialization Remote Code Execution Vulnera
  2. Cisco Secure Firewall Management Center Software sftunnel Root Arbitrary Code Execution Vulnerabilit
  3. CVE-2026-20242
  4. CVE-2026-20324

2.3.4 Zyxel GS1900系列交換器存在高風險安全漏洞(CVE-2026-7273)

CVE 編號	CVE-2026-7273
影響產品	Zyxel GS1900
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：

  研究人員發現 Zyxel GS1900 系列交換器存在重大資安漏洞(CVE-2026-7273，CVSS:8.8)，此為堆疊型緩衝區溢位(Stack-based Buffer Overflow)漏洞，未經身分鑑別之同一區網攻擊者可藉由向 CGI 程式傳送特製 HTTP 請求，觸發記憶體毀損，進而於受影響裝置執行作業系統指令，該漏洞已遭駭客濫用，請儘速確認並進行修補。

- 影響平台：
  - Zyxel GS1900-8 2.90(AAHH.1)C0(含)以前版本、
  - Zyxel GS1900-8HP 2.90(AAHI.1)C0(含)以前版本、
  - Zyxel GS1900-10HP 2.90(AAZI.1)C0(含)以前版本、
  - Zyxel GS1900-16 2.90(AAHJ.1)C0(含)以前版本、
  - Zyxel GS1900-24 2.90(AAHL.1)C0(含)以前版本、
  - Zyxel GS1900-24E 2.90(AAHK.1)C0(含)以前版本、
  - Zyxel GS1900-24EP 2.90(ABTO.1)C0(含)以前版本、
  - Zyxel GS1900-24HPv2 2.90(ABTP.1)C0(含)以前版本、
  - Zyxel GS1900-48 2.90(AAHN.1)C0(含)以前版本、
  - Zyxel GS1900-48HPv2 2.90(ABTQ.1)C0(含)以前版本
- 資料來源：
  1. Zyxel security advisory for stack-based buffer overflow vulnerability in GS1900 series switches
  2. CVE-2026-7273

2.3.5 Cisco Catalyst SD-WAN 存在重大資安漏洞(CVE-2026-76504)

CVE 編號	CVE-2026-76504
影響產品	Cisco Catalyst SD-WAN
解決辦法	請更新至以下版本： Cisco Catalyst SD-WAN Software 20.9.10.1 (含)之後版本、 Cisco Catalyst SD-WAN Software 20.12.8.2 (含)之後版本、 Cisco Catalyst SD-WAN Software 20.15.6.1 (含)之後版本、 Cisco Catalyst SD-WAN Software 20.18.4.1 (含)之後版本、 Cisco Catalyst SD-WAN Software 26.1.2.1 (含)之後版本、 Cisco Catalyst SD-WAN Software 26.2.1 (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-2026-76504，CVSS：9.8)，此為 API 身份驗證不當漏洞，允許遠端攻擊者繞過驗證進而取得管理者權限且以 API 存取系統。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：
  - Cisco Catalyst SD-WAN Software 20.9(含) 以前版本
  - Cisco Catalyst SD-WAN Software 20.12 版本
  - Cisco Catalyst SD-WAN Software 20.15 版本
  - Cisco Catalyst SD-WAN Software 20.18 版本
  - Cisco Catalyst SD-WAN Software 26.1 版本
  - Cisco Catalyst SD-WAN Software 26.2 版本

- 資料來源：
  1. Cisco Catalyst SD-WAN Manager API Authentication Bypass Vulnerability
  2. CVE-2026-76504

2.3.6 Microsoft Office SharePoint存在高風險安全漏洞(CVE-2026-65660)

CVE 編號	CVE-2026-65660
影響產品	Microsoft Office SharePoint
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置

- 內容說明：

  研究人員發現 Microsoft Office SharePoint 存在程式碼注入漏洞(CVE-2026-65660，CVSS：8.8)，此漏洞允許已通過身分驗證的遠端攻擊者可藉由傳送特製請求注入程式碼，進而執行任意程式碼，該漏洞已遭駭客濫用，請儘速確認並進行處置。

- 影響平台：
  - Microsoft SharePoint Enterprise Server 2016 16.0.5565.1001(不含)以前版本
  - Microsoft Sharepoint Server 2016 Language Pack Enterprise Edition 16.0.5565.1001(不含)以前版本
  - Microsoft SharePoint Server 2019 16.0.10417.20198 (不含)以前版本
  - Microsoft SharePoint Server Subion Edition 16.0.19725.20522(不含)以前版本
  - Microsoft Sharepoint Server Language Pack Subion Edition 16.0.19725.20522(不含)以前版本
- 資料來源：
  1. CVE-2026-65660

2.3.7 pgAdmin 4存在高風險安全漏洞(CVE-2026-86863)

CVE 編號	CVE-2026-86863
影響產品	pgAdmin 4
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置

- 內容說明：

  研究人員發現 pgAdmin 4 存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-86863，CVSS：9.8)，當啟用 Webserver 身分認證來源時，未經身分驗證的遠端攻擊者可藉由傳送特製 HTTP 請求標頭冒充任意使用者(包含管理者)，進而取得 pgAdmin 管理權限。

- 影響平台：
  - pgAdmin 4 之 6.2 至 9.17 版本
- 資料來源：
  1. Authentication bypass via a client-controlled identity header in Webserver authentication mode
  2. CVE-2026-86863

2.3.8 Check Point多項產品存在高風險安全漏洞(CVE-2026-93616)

CVE 編號	CVE-2026-93616
影響產品	Check Point Security Management Server、Multi-Domain Security Management Server、Log Server、Multi-Domain Log Server 及 SmartEvent
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置

- 內容說明：

  研究人員發現 Check Point Security Management Server、Multi-Domain Security Management Server、Log Server、Multi-Domain Log Server 及 SmartEvent 存在路徑遍歷漏洞(CVE-2026-93616，CVSS：9.8)，未經身分驗證的遠端攻擊者可利用路徑遍歷與檔案上傳缺陷上傳任意腳本，進而執行任意程式碼。該漏洞已遭駭客濫用，請儘速確認並進行處置。

- 影響平台：
  - R82.20 版本
  - R82.10 Jumbo Hotfix Take 44(含)以前版本
  - R82 Jumbo Hotfix Take 126(含)以前版本
  - R81.20 Jumbo Hotfix Take 166(含)以前版本
  - R81.10 Jumbo Hotfix Take 190(含)以前版本(已終止軟體維護)
  - R81、R80.40、R80.30、R80.20、R80.10 及 R80(已終止軟體維護)
- 資料來源：
  1. checkpoint CVE-2026-93616
  2. CVE-2026-93616

2.3.9 F5 BIG-IP APM存在高風險安全漏洞(CVE-2026-94127)

CVE 編號	CVE-2026-94127
影響產品	F5 BIG-IP APM
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置

- 內容說明：

  研究人員發現 F5 BIG-IP Access Policy Manager(APM)存在堆積型緩衝區溢位(Heap-based Buffer Overflow)漏洞(CVE-2026-94127，CVSS：9.8)，當 APM 設定為 OAuth 授權伺服器時，未經身分鑑別之遠端攻擊者可藉由傳送特定惡意流量，進而執行任意程式碼。該漏洞已遭駭客濫用，請儘速確認並進行處置。

- 影響平台：
  - BIG-IP APM 17.1.0 至 17.1.3、17.5.0 至 17.5.1 及 21.1.0 版本
- 資料來源：
  1. K000162605: BIG-IP APM vulnerability CVE-2026-94127
  2. CVE-2026-94127

2.3.10 SonicWall 旗下SMA1000系列產品存在重大資安漏洞 (CVE-2026-102255)

CVE 編號	CVE-2026-102255
影響產品	SonicWall SMA1000
解決辦法	請更新至以下版本： SMA 1000 系列產品 12.4.3-03670(含)之後版本、 SMA 1000 系列產品 12.5.0-03082(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-2026-102255，CVSS：10.0)，此為預先認證 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發出非預期請求，從而存取內部功能並執行未經授權的操作。

- 影響平台：
  - SMA 1000 系列產品 12.4.3-03526(含)之前版本
  - SMA 1000 系列產品 12.5.0-02952(含)之前版本
- 資料來源：
  1. SonicWall SMA1000 Series Appliances Affected By Multiple Vulnerabilities
  2. CVE-2026-102255

2.3.11 Veeam旗下Veeam Backup & Replication備份軟體存在重大資安漏洞 (CVE-2025-64393)

CVE 編號	CVE-2025-64393
影響產品	Veeam Backup & Replication
解決辦法	請更新至 Veeam Backup & Replication 12.3.2 P4 12.3.2.4934(含)之後版本

- 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(CVE-2025-64393，CVSS 4.x：9.4)公告。此漏洞允許具有 Backup Viewer 的低權限使用者，透過對透過掛載服務接收的不受信任的資料進行不安全的反序列化，在備份伺服器上執行遠端程式碼(RCE)。

- 影響平台：
  - Veeam Backup & Replication 12.3.2 P3 12.3.2.4854(含)之前版本
- 資料來源：
  1. Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2 P4
  2. CVE-2025-64393

2.3.12 Cisco 旗下 Nexus 3000 和 9000系列交換器存在4個重大資安漏洞

CVE 編號	CVE-2026-76465,CVE-2026-76485,CVE-2026-76486,CVE-2026-76501
影響產品	Cisco Nexus 3000 、 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 3000 和 9000 系列交換器發布重大資安漏洞公告 (CVE-2026-76465 、 CVE-2026-76485 、 CVE-2026-76486 、 CVE-2026-76501，CVSS 分數皆為 9.8)，皆為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，或導致受影響的裝置出現 DoS 攻擊。

- 影響平台：
  - Nexus 3000 Series Switches
  - Nexus 9000 Series Switches in standalone NX-OS mode
  - Nexus 3000 Series Switches 和 Nexus 9000 Series Switches 啟用 NGOAM 並設定其設定功能，詳見官方網站說明
- 資料來源：
  1. Cisco Nexus 3000 and 9000 Series Switches MPLS OAM Remote Code Execution Vulnerability
  2. Cisco Nexus 3000 and 9000 Series Switches NGOAM Remote Code Execution Vulnerabilities
  3. CVE-2026-76465
  4. CVE-2026-76485
  5. CVE-2026-76486
  6. CVE-2026-76501

2.3.13 Splunk Enterprise存在高風險安全漏洞(CVE-2026-76268)，請儘速確認並進行處置

CVE 編號	CVE-2026-76268
影響產品	Splunk Enterprise
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置

- 內容說明：

  研究人員發現 Splunk Enterprise 存在缺乏身分鑑別(Missing Authentication)漏洞(CVE-2026-76268，CVSS：9.8)。未經身分驗證的遠端攻擊者，可利用 Search Head 叢集成員之 Patroni REST API 對關鍵組態操作未要求身分識別之缺陷，進而執行任意作業系統指令。

- 影響平台：
  - Splunk Enterprise 10.4.0 至 10.4.2 版本
  - Splunk Enterprise 10.2.0 至 10.2.6 版本
- 資料來源：
  1. Security Vulnerabilities in Splunk Enterprise - September/October 2026
  2. CVE-2026-76268

2.3.14 Ivanti Neurons for Intune 存在重大資安漏洞(CVE-2026-109412)

CVE 編號	CVE-2026-109412
影響產品	Ivanti Neurons for Intune
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：

  Ivanti 針對 Ivanti Neurons Patch for Intune 發布重大資安漏洞公告(CVE-2026-109412，CVSS：9.9)，此漏洞允許經身分驗證的遠端攻擊者可洩漏敏感身分驗證資訊。

- 影響平台：
  - Ivanti Neurons Patch for Intune
- 資料來源：
  1. Security Advisory Ivanti Neurons Patch for Intune October 2026 (CVE-2026-109412)
  2. CVE-2026-109412

2.3.15 Ivanti旗下Xtraction存在高風險資安漏洞(CVE-2026-106042)

CVE 編號	CVE-2026-106042
影響產品	Ivanti Xtraction
解決辦法	請更新至 Ivanti Xtraction 2026.4(含)之後版本

- 內容說明：

  Ivanti 旗下的 Xtraction 是一套 IT 報表與資料視覺化平台，可將不同 IT 系統的資料整合至同一儀表板，方便即時查看與分析。近期 Ivanti 發布重大資安漏洞公告(CVE-2026-106042，CVSS：9.9)。此漏洞允許經身分驗證的攻擊者將應用程式產生的請求導向到攻擊者控制的端點，並取得應用程式傳輸的 EPMM 連接器憑證。

- 影響平台：
  - Ivanti Xtraction 2026.2.1(含)以前版本
- 資料來源：
  1. Security Advisory Ivanti Xtraction (Multiple CVEs)
  2. CVE-2026-106042

2.3.16 FortiSIEM 存在重大資安漏洞(CVE-2026-106173)

CVE 編號	CVE-2026-106173
影響產品	Fortinet FortiSIEM
解決辦法	請將 FortiSIEM 更新至 7.5.1(含)之後版本

- 內容說明：

  Fortinet 針對 FortiSIEM 發布重大資安漏洞公告(CVE-2026-106173，CVSS：9.8)。此漏洞可能允許未經身分驗證的攻擊者，透過精心設計的資料執行未經授權的程式碼或命令。

- 影響平台：
  - FortiSIEM 7.5.0 版本
- 資料來源：
  1. Arbitrary file write in grpc phQueryMaster
  2. CVE-2026-106173

2.3.17 FortiSandbox GUI 存在重大資安漏洞(CVE-2026-107656)

CVE 編號	CVE-2026-107656
影響產品	Fortinet FortiSandbox GUI
解決辦法	請更新至以下版本： FortiSandbox 5.0.7 (含)之後版本、 FortiSandbox 4.4.10 (含)之後版本、 FortiSandbox PaaS 5.0.7(含)之後版本、

- 內容說明：

  Fortinet 針對 FortiSandbox GUI 發布重大資安漏洞公告(CVE-2026-107656，CVSS：9.6)。此漏洞可能允許未經身分驗證的攻擊者，透過精心建構的 HTTP 請求繞過身分驗證。

- 影響平台：
  - FortiSandbox 5.0.0 至 5.0.6 版本
  - FortiSandbox 4.4.0 至 4.4.9 版本
  - FortiSandbox PaaS 5.0.0 至 5.0.6 版本
  - FortiSandbox PaaS 4.4 版本
- 資料來源：
  1. Improper access control and session management in the web management interface

2.3.18 FortiAnalyzer、FortiManager、FortiManager Cloud 和 FortiAnalyzer Cloud 存在重大資安漏洞(CVE-2025-46773)

CVE 編號	CVE-2025-46773
影響產品	Fortinet FortiAnalyzer、FortiManager、FortiManager Cloud、FortiAnalyzer Cloud
解決辦法	請更新至以下版本： FortiAnalyzer 7.6.5 版本 FortiAnalyzer 7.4.8 版本 FortiAnalyzer Cloud 7.6.5 版本 FortiAnalyzer Cloud 7.4.8 版本 FortiAnalyzer Cloud 7.2.12 版本 FortiManager 7.6.5 版本 FortiManager 7.4.7 版本 FortiManager Cloud 7.6.5 版本

- 內容說明：

  Fortinet 針對 FortiAnalyzer、FortiManager、FortiManager Cloud 和 FortiAnalyzer Cloud 發布重大資安漏洞公告(CVE-2025-46773，CVSS：8.8)。此為 SQL 注入漏洞，因特殊元素未適當處理，可能允許低權限使用者透過精心設計的請求執行任意指令。

- 影響平台：
  - FortiAnalyzer 7.6.0 至 7.6.4 版本
  - FortiAnalyzer 7.4.0 至 7.4.7 版本
  - FortiAnalyzer 7.2 版本
  - FortiAnalyzer Cloud 7.6.2 至 7.6.4 版本
  - FortiAnalyzer Cloud 7.4.1 至 7.4.7 版本

- FortiAnalyzer Cloud 7.2.1 至 7.2.11 版本
- FortiManager 7.6.0 至 7.6.4 版本
- FortiManager 7.4.0 至 7.4.6 版本
- FortiManager 7.2 版本
- FortiManager Cloud 7.6.2 至 7.6.4 版本

- 資料來源：
  1. Multiple Arbitrary File Read/Write via SQL Injection
  2. CVE-2025-46773

2.3.19 Cisco License (Smart Software Manager) On-Prem 存在2個重大資安漏洞

CVE 編號	CVE-2026-20328,CVE-2026-76454
影響產品	Cisco License (Smart Software Manager) On-Prem
解決辦法	請更新至 Cisco License On-Prem 10-202608 (含)之後版本

- 內容說明：

  Cisco 針對旗下 License (Smart Software Manager) On-Prem 發布重大資安漏洞公告(CVE-2026-20328、CVE-2026-76454，CVSS 分數皆為 9.1)。

  【CVE-2026-76454】

  此漏洞存在於 Cisco Smart Licensing Utility API，可能允許未經身份驗證的遠端攻擊者可在系統寫入任意文件，或導致受影響的應用程式出現 DoS 攻擊。

  【CVE-2026-20328】

  此漏洞存在於 Web 管理介面，可能允許未經身份驗證的遠端攻擊者取得受影響應用程式的未經授權的存取。

- 影響平台：
  - Cisco License On-Prem 9-202601(含)之前版本
  - Cisco License On-Prem 10-202608(不含)之前版本
- 資料來源：
  1. Cisco License (Smart Software Manager) On-Prem Vulnerabilities
  2. CVE-2026-20328
  3. CVE-2026-76454

2.3.20 Cisco NX-OS Software NX-API 存在重大資安漏洞(CVE-2026-76471)

CVE 編號	CVE-2026-76471
影響產品	Cisco NX-OS Software NX-API
解決辦法	請更新至 UCS 6300 Series Fabric Interconnect Cisco UCS Software 4.3(6j) (含)之後版本

- 內容說明：

  Cisco 針對旗下 NX-OS Software NX-API 發布重大資安漏洞公告(CVE-2026-76471，CVSS：9.8)。此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，或導致受影響的裝置出現 DoS 攻擊。

- 影響平台：
  - UCS 6300 Series Fabric Interconnect Cisco UCS Software 4.2(含)之前版本
  - UCS 6300 Series Fabric Interconnect Cisco UCS Software 4.3 版本
- 資料來源：
  1. Cisco NX-OS Software NX-API Remote Code Execution Vulnerability
  2. CVE-2026-76471

2.3.21 SonicWall NSM On-Prem 存在重大資安漏洞(CVE-2026-96540)

CVE 編號	CVE-2026-96540
影響產品	SonicWall NSM On-Prem
解決辦法	請將 Network Security Manager (NSM) On-Prem 更新至 4.4.0 (含)之後版本

- 內容說明：

  SonicWall 針對 NSM On-Prem 發布重大資安漏洞(CVE-2026-96540，CVSS：8.8)。此為存取控制漏洞，可能允許經身分驗證的攻擊者取取得敏感資訊。攻擊者可利用此漏洞將權限提升至管理員，或攔截 NSM instance 其他使用者通訊。

- 影響平台：
  - Network Security Manager (NSM) On-Prem 4.3.1 (含)以前版本
- 資料來源：
  1. CVE-2026-96540
  2. SonicWall NSM On-Prem Affected By Multiple Vulnerabilities

2.3.22 Cisco Secure Email Gateway 存在重大資安漏洞(CVE-2026-76519)

CVE 編號	CVE-2026-76519
影響產品	Cisco Secure Email Gateway
解決辦法	請更新至以下版本： Cisco AsyncOS Software for Cisco Secure Email Gateway 15.5.5-014 版本、 Cisco AsyncOS Software for Cisco Secure Email Gateway 16.5.0-780 版本

- 內容說明：

  Cisco 針對 Cisco Secure Email Gateway 發布重大資安漏洞(CVE-2026-76519，CVSS：9.8)。此漏洞存在於 Advanced Malware Protection (AMP)，可能允許未經身分驗證的遠端攻擊者，在底層作業系統上寫入任意檔案。

- 影響平台：
  - Cisco AsyncOS Software for Cisco Secure Email Gateway 15.5 版本
  - Cisco AsyncOS Software for Cisco Secure Email Gateway 16.0 版本
  - Cisco AsyncOS Software for Cisco Secure Email Gateway 16.5 版本
- 資料來源：
  1. CVE-2026-76519
  2. Cisco Secure Email Gateway Arbitrary File Write Vulnerability

2.3.23 Cisco License (Smart Software Manager) On-Prem 存在4個重大資安漏洞

CVE 編號	CVE-2026-76480,CVE-2026-76482,CVE-2026-76483,CVE-2026-76484
影響產品	Cisco License (Smart Software Manager) On-Prem
解決辦法	請更新至 Cisco License On-Prem 10-202609 (含)之後版本

- 內容說明：

  Cisco License (Smart Software Manager) On-Prem 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-2026-76480，CVSS：9.8，關鍵功能缺少身分驗證。

  CVE-2026-76482，CVSS：10.0，對加密簽章驗證不當。

  CVE-2026-76483，CVSS：9.1，憑證保護不足。

  CVE-2026-76484，CVSS：8.8，程式碼注入攻擊。

- 影響平台：
  - Cisco License On-Prem 9-202601(含)之前版本
  - Cisco License On-Prem 10-202608(含)之前版本
- 資料來源：
  1. Cisco License (Smart Software Manager) On-Prem Security Hardening Release: October 2026
  2. CVE-2026-76480
  3. CVE-2026-76482
  4. CVE-2026-76483
  5. CVE-2026-76484

2.3.24 Cisco NX-OS Software NX-API 存在3個重大資安漏洞

CVE 編號	CVE-2026-76453,CVE-2026-76455,CVE-2026-76459
影響產品	Cisco NX-OS Software NX-API
解決辦法	請更新至以下版本： MDS 9000 Series Multilayer Switches Cisco NX-OS Software 9.4(5a)(含)之後版本、 Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode Cisco NX-OS Software 10.3(10)(含)之後版本、 Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode Cisco NX-OS Software 10.4(8)(含)之後版本、 Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode Cisco NX-OS Software 10.5(6)(含)之後版本、 Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode Cisco NX-OS Software 10.6(4)(含)之後版本、 Nexus 7000 Series Switches Cisco NX-OS Software 8.4(14)(含)之後版本、 Nexus 9000 Series Fabric Switches in ACI mode Cisco NX-OS Software 16.0(9h)(含)之後版本、 Nexus 9000 Series Fabric Switches in ACI mode Cisco NX-OS Software 16.1(6g)(含)之後版本、 Nexus 9000 Series Fabric Switches in ACI mode Cisco NX-OS Software 16.2(3g)(含)之後版本、

	UCS 6300, 6400, 6500, and 6600 Series and 9108 100G Fabric Interconnects UCS Manager Managed Mode 4.3(6j)(含)之後版本、 UCS 6300, 6400, 6500, and 6600 Series and 9108 100G Fabric Interconnects UCS Manager Managed Mode 6.0(2e)(含)之後版本、 UCS 6300, 6400, 6500, and 6600 Series and 9108 100G Fabric Interconnects UCS Intersight Managed Mode 4.3(6.260049)(含)之後版本、 UCS 6300, 6400, 6500, and 6600 Series and 9108 100G Fabric Interconnects UCS Intersight Managed Mode 4.3(6.260059)(含)之後版本、 UCS 6300, 6400, 6500, and 6600 Series and 9108 100G Fabric Interconnects UCS Intersight Managed Mode 6.0(2.260080)(含)之後版本

- 內容說明：

  Cisco NX-OS 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-2026-76453，CVSS：8.8，為不適當處理漏洞。

  CVE-2026-76455，CVSS：9.8，為存取控制不當漏洞。

  CVE-2026-76459，CVSS：9.8，為越界寫入漏洞。

- 影響平台：
  - MDS 9000 Series Multilayer Switches Cisco NX-OS Software 9.3(含)之前版本
  - MDS 9000 Series Multilayer Switches Cisco NX-OS Software 9.4 版本
  - Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode Cisco NX-OS Software 10.3(含)之前版本

- Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode Cisco NX-OS Software 10.4 版本
- Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode Cisco NX-OS Software 10.5 版本
- Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode Cisco NX-OS Software 10.6 版本
- Nexus 7000 Series Switches Cisco NX-OS Software 8.3(含)之前版本
- Nexus 7000 Series Switches Cisco NX-OS Software 8.4 版本
- Nexus 9000 Series Fabric Switches in ACI mode Cisco NX-OS Software 16.0(含)之前版本
- Nexus 9000 Series Fabric Switches in ACI mode Cisco NX-OS Software 16.1 版本
- Nexus 9000 Series Fabric Switches in ACI mode Cisco NX-OS Software 16.2 版本
- UCS 6300, 6400, 6500, and 6600 Series and 9108 100G Fabric Interconnects Cisco UCS Software 4.2(含)之前版本
- UCS 6300, 6400, 6500, and 6600 Series and 9108 100G Fabric Interconnects Cisco UCS Software 4.3 版本
- UCS 6300, 6400, 6500, and 6600 Series and 9108 100G Fabric Interconnects Cisco UCS Software 6.0 版本

- 資料來源：
  1. Cisco NX-OS Software Security Hardening Release: October 2026
  2. CVE-2026-76453
  3. CVE-2026-76455
  4. CVE-2026-76459

2.3.25 Cisco Application Policy Infrastructure Controller 存在3個重大資安漏洞

CVE 編號	CVE-2026-76498,CVE-2026-76499,CVE-2026-76500
影響產品	Cisco Application Policy Infrastructure Controller
解決辦法	請更新至以下版本： Cisco APIC 6.0 (9h) (含)之後版本、 Cisco APIC 6.1 (6g) (含)之後版本、 Cisco APIC 6.2 (3g) (含)之後版本

- 內容說明：

  Cisco Application Policy Infrastructure Controller 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-2026-76498，CVSS：9.8，為存取控制不當漏洞。

  CVE-2026-76499，CVSS：9.8，為不適當處理漏洞。

  CVE-2026-76500，CVSS：9.8，在產品的生命週期內存在不當控制。

- 影響平台：
  - Cisco APIC 5.3 (含)之前版本
  - Cisco APIC 6.0 版本
  - Cisco APIC 6.1 版本
  - Cisco APIC 6.2 版本
- 資料來源：
  1. Cisco Application Policy Infrastructure Controller Security Hardening Release: October 2026
  2. CVE-2026-76498
  3. CVE-2026-76499
  4. CVE-2026-76500

2.3.26 Cisco Meraki 存在 4 個重大資安漏洞

CVE 編號	CVE-2026-76463,CVE-2026-76464,CVE-2026-76470,CVE-2026-76472
影響產品	Cisco Meraki
解決辦法	請更新至以下版本： Cisco Meraki Campus Gateway 32.2.5 (含)之後版本、 Cisco Meraki Campus Gateway 33.1.4 (含)之後版本、 Cisco Meraki MG Cellular Gateway 26.1.4 (含)之後版本、 Cisco Meraki MR Wireless Access Point Software 30.7.3 (含)之後版本、 Cisco Meraki MR Wireless Access Point Software 31.1.8.1(含)之後版本、 Cisco Meraki MR Wireless Access Point Software 32.2.5 (含)之後版本、 Cisco Meraki MR Wireless Access Point Software 33.1.3 (含)之後版本、 Cisco Meraki MS Series Switch Software 18.1.9 (含)之後版本、 Cisco Meraki MS Series Switch Software IOS XE 17.15.6 (含)之後版本、 Cisco Meraki MS Series Switch Software IOS XE 17.18.4.1 (含)之後版本、 Cisco Meraki MS Series Switch Software IOS XE 26.1.2 (含)之後版本、 Cisco Meraki MV Smart Camera 8.0 (含)之後版本、

	Cisco Meraki MX Security and SD-WAN Appliance 18.107.14 (含)之後版本、 Cisco Meraki MX Security and SD-WAN Appliance 19.2.9 (含)之後版本、 Cisco Meraki MX Security and SD-WAN Appliance 26.1.7 (含)之後版本、 Cisco Meraki MX Security and SD-WAN Appliance 26.2.3 (含)之後版本

- 內容說明：

  Cisco Meraki 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-2026-76463，CVSS：8.8，為存取控制不當漏洞。

  CVE-2026-76464，CVSS：9.6，記憶體緩衝區的操作限制不當。

  CVE-2026-76470，CVSS：8.8，為計算錯誤。

  CVE-2026-76472，CVSS：8.8，為特殊元素未適當處理。

- 影響平台：
  - Cisco Meraki Campus Gateway 32.2 版本
  - Cisco Meraki Campus Gateway 33.1 版本
  - Cisco Meraki MG Cellular Gateway 26.1 版本
  - Cisco Meraki MR Wireless Access Point Software 30.7 版本
  - Cisco Meraki MR Wireless Access Point Software 31.1 版本
  - Cisco Meraki MR Wireless Access Point Software 32.2 版本
  - Cisco Meraki MR Wireless Access Point Software 33.1 版本
  - Cisco Meraki MS Series Switch Software 18.1 版本
  - Cisco Meraki MS Series Switch Software IOS XE 17.15 版本

- Cisco Meraki MS Series Switch Software IOS XE 17.18 版本
- Cisco Meraki MS Series Switch Software IOS XE 26.1 版本
- Cisco Meraki MV Smart Camera 7 版本
- Cisco Meraki MX Security and SD-WAN Appliance 18.1 版本
- Cisco Meraki MX Security and SD-WAN Appliance 19.2 版本
- Cisco Meraki MX Security and SD-WAN Appliance 26.1 版本
- Cisco Meraki MX Security and SD-WAN Appliance 26.2 版本

- 資料來源：
  1. Cisco Meraki Security Hardening Release: October 2026
  2. CVE-2026-76463
  3. CVE-2026-76464
  4. CVE-2026-76470
  5. CVE-2026-76472

2.3.27 Dell System Update存在高風險安全漏洞(CVE-2026-86360)，請儘速確認並進行處置

CVE 編號	CVE-2026-86360
影響產品	Dell System Update
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置。

- 內容說明：

  研究人員發現 Dell System Update 存在路徑遍歷(Path Traversal)漏洞(CVE-2026-86360，CVSS：9.6)，未經身分鑑別之遠端攻擊者可利用此漏洞存取檔案系統，進而以 root 權限執行任意程式碼，請儘速確認並進行處置。

- 影響平台：
  - Dell System Update 2.3.0.0(不含)以前版本
- 資料來源：
  1. DSA-2026-324: Security update for Dell System Update (DSU) Vulnerabilities
  2. CVE-2026-86360

2.3.28 GitLab AI Gateway存在高風險安全漏洞(CVE-2026-90970)，請儘速確認並進行處置

CVE 編號	CVE-2026-90970
影響產品	GitLab AI Gateway
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置。

- 內容說明：

  研究人員發現 GitLab AI Gateway 存在沙箱逃逸(Sandbox Escape)漏洞(CVE-2026-90970，CVSS：9.9)，具 Duo Agent Platform 流程組態與範本設定權限且已通過身分鑑別之遠端攻擊者，可透過提交特製之提示範本逃脫提示範本沙箱限制，進而於 AI Gateway 上執行任意指令，請儘速確認並進行處置。

- 影響平台：
  - GitLab AI Gateway 18.1.6 至 19.2.4(不含)、19.3.0 至 19.3.2(不含)及 19.4.0 至 19.4.1(不含)版本
- 資料來源：
  1. GitLab AI Gateway Critical Patch Release: 19.2.4, 19.3.2, and 19.4.1
  2. CVE-2026-90970

2.3.29 PHP 存在2個重大資安漏洞(CVE-2026-109618 和 CVE-2026-109619)

CVE 編號	CVE-2026-109618,CVE-2026-109619
影響產品	PHP
解決辦法	官方將針對漏洞釋出修補或更新，建議系統管理者儘速將 PHP 升級至下列受支援之最新安全版本： PHP 8.5.12 PHP 8.4.27 PHP 8.3.36 PHP 8.2.35 註：PHP 8.1(含)以下版本因官方已停止維護(EOL)，將不會獲得官方修補更新，建議儘速升級至上述仍支援之版本。

- 內容說明：

  PHP 發布重大資安漏洞公告（CVE-2026-109618 和 CVE-2026-109619，CVSS 4.x 分數皆為 9.2），網路上已出現本漏洞概念驗證程式（PoC），請儘速確認並進行處置。

  【CVE-2026-109618】

  此為使用釋放後記憶體（Use After Free）漏洞，與記憶體不足（Out of Memory, OOM）處理有關，可能因記憶體未完全初始化，導致未經身分驗證的遠端攻擊者，可透過傳送特製的 http 請求，在受影響的伺服器上執行任意程式碼（RCE）。

  【CVE-2026-109619】

  此為使用釋放後記憶體（Use After Free）漏洞，可能因全域狀態未完全初始化，導致未經身分驗證的遠端攻擊者，可透過傳送特製的 http 請求，在受影響的伺服器上執行任意程式碼（RCE）。

- 影響平台：
  - PHP 5.4.x 至 5.6.x 之所有版本

- PHP 7.0.x 至 7.4.x 之所有版本
- PHP 8.0.x 至 PHP 8.1.x 之所有版本
- PHP 8.5.11(含)以下版本
- PHP 8.4.26(含)以下版本
- PHP 8.3.35(含)以下版本
- PHP 8.2.34(含)以下版本

- 資料來源：
  1. Security advisory: Critical remote code execution vulnerabilities, update now
  2. Downloads & Installation Instructions
  3. CVE-2026-109618
  4. CVE-2026-109619

2.3.30 Node.js 存在4個重大資安漏洞，請儘速確認並進行處置

CVE 編號	CVE-2026-105482,CVE-2026-105483,CVE-2026-106069,CVE-2026-111497
影響產品	Node.js
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置

- 內容說明：

  研究人員發現 Node.js 存在 4 個重大資安漏洞（CVE-2026-105482、CVE-2026-105483、CVE-2026-106069 及 CVE-2026-111497），類型包含空字元輸入驗證不足、TLS 憑證主機名稱檢查繞過(TLS Certificate Hostname Bypass)及越界寫入(Out-of-Bounds Write)，請儘速確認並進行處置。

  【CVE-2026-105482】

  dns.resolve 函式處理含 NUL 字元之名稱時，會將名稱截斷。

  【CVE-2026-105483】

  Node.js 24.x 與 26.x 版本中，當 IP 位址以全形書寫時，攻擊者可繞過 TLS 憑證之主機名稱檢查。

  【CVE-2026-106069】

  當主機名稱為非標準格式之 IP 位址時，攻擊者可繞過 TLS 憑證之主機名稱檢查。

  【CVE-2026-111497】

  Brotli 解碼器存在越界寫入缺陷，可導致遠端執行程式碼。

- 影響平台：
  - Node.js 22.0.0 至 22.23.4(不含)版本
  - Node.js 24.0.0 至 24.22.1(不含)版本
  - Node.js 26.0.0 至 26.12.1(不含)版本

- 資料來源：
  1. Wednesday, October 21, 2026 Security Releases

2.3.31 GitLab存在2項高風險安全漏洞(CVE-2026-97229與CVE-2026-110264)

CVE 編號	CVE-2026-97229,CVE-2026-110264
影響產品	GitLab CE/EE
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下： https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/ https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/

- 內容說明：

  研究人員發現 GitLab 社群版(CE)與企業版(EE)存在 2 項整數溢位(Integer Overflow)漏洞(CVE-2026-97229 與 CVE-2026-110264)，請儘速確認使用版本並並進行處置。

  【CVE-2026-97229】

  此漏洞於特定條件下，未經身分鑑別之遠端攻擊者可藉由於 CI/CD 組態中使用特製之正規表示式，進而於 GitLab 伺服器執行任意程式碼。

  【CVE-2026-110264】

  此漏洞因編譯特製之正規表示式時發生整數溢位，於特定條件下，未經身分鑑別之遠端攻擊者可於 GitLab 伺服器執行任意程式碼。

- 影響平台：
  - GitLab CE/EE 7.0 至 18.11.13(不含)、19.0 至 19.0.10(不含)、19.1 至 19.1.9(不含)、19.2 至 19.2.9(不含)、19.3 至 19.3.6(不含)、19.4 至 19.4.3(不含)及 19.5 至 19.5.1(不含)版本

- 資料來源：
  1. GitLab Critical Patch Release: 19.4.2, 19.3.5, 19.2.8
  2. GitLab Critical Patch Release: 19.5.1, 19.4.3, 19.3.6, 19.2.9, 19.1.9, 19.0.10, 18.11.13
  3. CVE-2026-97229
  4. CVE-2026-110264

2.3.32 Oracle Java SE與Oracle GraalVM存在高風險安全漏洞(CVE-2026-91403)，請儘速確認並進行處置

CVE 編號	CVE-2026-91403
影響產品	Oracle Java SE、Oracle GraalVM
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下： https://www.oracle.com/security-s/-cve-2026-91403.html

- 內容說明：

  研究人員發現 Oracle Java SE、Oracle GraalVM for JDK 及 Oracle GraalVM Enterprise Edition 之 JSSE 元件存在高風險安全漏洞(CVE-2026-91403)，未經身分鑑別之遠端攻擊者可透過多種通訊協定進行攻擊，進而未經授權存取、新增、刪除或修改重要資料，請儘速確認並進行處置。

- 影響平台：
  - Oracle Java SE 之 8u511、8u511-perf、11.0.33、17.0.21、21.0.13、25.0.5 及 27.0.1 版本
  - Oracle GraalVM for JDK 之 17.0.21 與 21.0.13 版本
  - Oracle GraalVM Enterprise Edition 21.3.20 版本建議處置
- 資料來源：
  1. Oracle Security Alert Advisory - CVE-2026-91403
  2. CVE-2026-91403

2.3.33 Go存在高風險安全漏洞(CVE-2026-111943)，請儘速確認並進行處置

CVE 編號	CVE-2026-111943
影響產品	Go
解決辦法	官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下： https://groups.google.com/g/golang-announce/c/66pojueaQek

- 內容說明：

  研究人員發現 Go 之 crypto/x509 套件存在不當憑證驗證(Improper Certificate Validation)漏洞(CVE-2026-111943)，因部分情況下系統信任憑證儲存區可能未即時更新，Certificate.Verify 函式可能接受含已撤銷或不受信任之中繼憑證授權中心(Intermediate CA)簽發之憑證鏈，攻擊者可藉此進行中間人攻擊，請儘速確認並進行處置。

- 影響平台：
  - Go 1.26.10(不含)以前版本
  - Go 1.27.0 至 1.27.3(不含)版本
- 資料來源：
  1. [security] Go 1.27.3 and Go 1.26.10 are released
  2. CVE-2026-111943

2.3.34 Fortinet 多款資安產品釋出安全強化更新，請儘速確認並完成更新

CVE 編號	
影響產品	Fortinet FortiOS、FortiManager、FortiAnalyzer、FortiMail、FortiAuthenticator
解決辦法	FortiOS：8.0.2、7.6.8、7.4.13、7.2.14 或以上版本 FortiManager：8.0.2、7.6.8、7.4.12、7.2.13 或以上版本 FortiAnalyzer：8.0.2、7.6.8、7.4.12、7.2.13 或以上版本 FortiMail：8.0.2、7.6.7、7.4.9 或以上版本；使用 7.2 分支者，應升級至 7.4 或以上分支 FortiAuthenticator：8.0.4、6.6.11 或以上版本 註 1. 儘速盤點相關設備及軟體版本，優先處理對外連網設備。 註 2. 依原廠建議完成更新，更新前應先備份設定，並確認更新後設備運作正常。 註 3. 如暫時無法更新，應限制管理介面對網際網路之存取，僅允許可信任 IP 連線；必要時採取網路隔離或其他適當防護措施，以降低遭受攻擊之風險。

- 內容說明：

  網路安全設備廠商 Fortinet 預定於 115 年 10 月 22 日發布多款產品安全強化更新，涵蓋 FortiOS、FortiManager、FortiAnalyzer、FortiMail 及 FortiAuthenticator 等 5 大系列，包含重大及高風險漏洞修補。為降低資安風險，請各單位儘速盤點所使用之相關產品及版本，優先更新對外連網設備，以維護企業資通安全。

  Fortinet 表示，本次漏洞係透過 AI 輔助安全測試計畫所發現，相關漏洞技術細節預計於 115 年 11 月 10 日公布。考量漏洞細節公開後可能

增加遭攻擊風險，請各單位及早完成更新準備，並於修補版本發布後儘速辦理升級。

- 影響平台：
  - FortiOS 7.2.0–7.2.13、7.4.0–7.4.12、7.6.0–7.6.7、8.0.0–8.0.1
  - FortiManager 7.2.0–7.2.12 、 7.4.0–7.4.11 、 7.6.0–7.6.7 、 8.0.0–8.0.1
  - FortiAnalyzer 7.2.0–7.2.12 、 7.4.0–7.4.11 、 7.6.0–7.6.7 、 8.0.0–8.0.1
  - FortiMail 7.2.0–7.2.9、7.4.0–7.4.8、7.6.0–7.6.6、8.0.0–8.0.1
  - FortiAuthenticator 6.6.0–6.6.10、8.0.0–8.0.3
- 資料來源：
  1. Fortinet Releases Security Hardening Release for Multiple Products

第 3 章、資安研討會及活動

- **資安研討會**

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】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	**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/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
2026 台灣資安通報應變年會：迎戰AI威脅 強化智慧應變	
活動時間	**2026年11月03日 09:30-16:20**
活動地點	**臺大醫院國際會議中心 401廳(台北市中正區徐州路2號4樓)**
活動網站	**https://activity.twcert.org.tw/2026/index.htm**

活動概要	 **【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】** 為協助資通安全管理法納管對象以外的民間企業提升資安防護量能，數位發展部責成國家資通安全研究院，自 2024 年 1 月接手營運台灣電腦網路危機處理暨協調中心(TWCERT/CC)，提供全年 24 小時不間斷的資安事件通報、情資分享、應變協調、國際合作及意識提升等各項企業資安服務工作。 由 TWCERT/CC 主辦之台灣資安通報應變年會邁入第十屆，本屆年會以「迎戰 AI 威脅　強化智慧應變」為主題，匯聚產官學各界資安專家，透過 AI 應用安全、智慧化攻防與人機協作等 AI 資安治理議題深入分享與交流，盼能加深企業對 AI 時代資安風險、實務應用及應變策略的理解，並將 AI 安全觀念落實於防禦策略、事件應變及治理機制之中，全面提升面對新型態資安威脅之應變能力，共同打造更安全、更具韌性的數位環境。 **【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**

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：

網擎資訊｜SecuShare Pro - OS Command Injection	
TVN / CVE ID	TVN-202610001 / CVE-2026-107459
CVSS	9.3 (Critical) CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 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	SecuShare Pro v4
問題描述	網擎資訊開發之SecuShare Pro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	雲端版：MailCloud（含 EaaS）環境已全數完成更新，服務不受影響，使用者無需採取額外措施。 標準版：SecuShare Pro 用戶請聯繫網擎資訊技術服務團隊協助進行版本更新。 客製版：請確認目前使用之系統版本，並將版號提供予網擎資訊，由網擎資訊提供對應之安全性更新程式。
公開日期	2026-10-08
相關連結	https://www.twcert.org.tw/tw/cp-132-11254-9c206-1.html
互動資通｜TeamPlus Messenger - 存在2個漏洞	
TVN / CVE ID	TVN-202610002 / CVE-2026-110444, CVE-2026-110445
CVSS	【CVE-2026-110444】

	8.6 (High) CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 8.8 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H 【CVE-2026-110445】 8.6 (High) CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 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	TeamPlus Messenger v16.8.0至v17.0.6版本
問題描述	【CVE-2026-110444(Code Injection)】 未經身分鑑別之遠端攻擊者可誘使使用者開啟特製連結，注入並執行任意JavaScript，進而在使用者確認安全警告後，以目前使用者權限執行任意程式碼。 【CVE-2026-110445(Code Injection)】 未經身分鑑別之遠端攻擊者可誘使使用者與特製內容互動，注入並執行任意JavaScript，進而在使用者確認安全警告後，以目前使用者權限執行任意程式碼。
解決方法	TeamPlus Messenger v17.0.7(含)以後
公開日期	2026-10-14
相關連結	https://www.twcert.org.tw/tw/cp-132-11270-88d86-1.html
凱發科技｜WebITR - Insecure Deserialization	
TVN / CVE ID	TVN-202610005 / CVE-2026-113404
CVSS	8.7 (High) CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 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	WebITR 2_1_0_34(含)以前版本
問題描述	凱發科技開發之WebITR差勤系統存在Insecure Deserialization漏洞，已通過身分鑑別之遠端攻擊者可利用硬編碼加密金鑰產生並傳送惡意序列化資料，進而於伺服器端執行任意程式碼。
解決方法	更新至2_1_0_36(含)以後版本
公開日期	2026-10-20
相關連結	https://www.twcert.org.tw/tw/cp-132-11296-d3d95-1.html
亞璿資訊｜BA-Workflow 工作流程表單平台 - 存在3個漏洞	
TVN / CVE ID	TVN-202610007 / CVE-2026-113405, CVE-2026-113406, CVE-2026-113407
CVSS	【CVE-2026-113405】 8.7 (High) CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 【CVE-2026-113406】 8.7 (High) CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 【CVE-2026-113407】 8.7 (High) CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N 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	【CVE-2026-113405, CVE-2026-113406】 BA-Workflow v3.6(不含)以前版本 【CVE-2026-113407】 BA-Workflow v3.6.2.7(不含)以前版本

問題描述	【CVE-2026-113405(SQL Injection)】 亞璿資訊BA-Workflow存在SQL Injection漏洞，已取得一般權限之遠端攻擊者可注入任意SQL指令，進而讀取、修改及刪除資料庫內容。 【CVE-2026-113406(SQL Injection)】 亞璿資訊BA-Workflow存在SQL Injection漏洞，已取得一般權限之遠端攻擊者可注入任意SQL指令，進而讀取、修改及刪除資料庫內容。 【CVE-2026-113407(SQL Injection)】 亞璿資訊BA-Workflow存在SQL Injection漏洞，已取得一般權限之遠端攻擊者，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v3.6.2.7(含)以後版本
公開日期	2026-10-20
相關連結	https://www.twcert.org.tw/tw/cp-132-11298-d9dd5-1.html
新人類資訊科技｜NT OneAPP企業雲端管理系統 - 存在5個漏洞	
TVN / CVE ID	TVN-202610006 / CVE-2026-114219, CVE-2026-114220, CVE-2026-114221, CVE-2026-114222, CVE-2026-114223
CVSS	【CVE-2026-114219】 9.1 (Critical) CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N 7.4 (High) CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N 【CVE-2026-114220】 9.3 (Critical) CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N 9.1 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

	【CVE-2026-114221】 5.9 (Medium) CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N 7.4 (High) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N 【CVE-2026-114222】 6.9 (Medium) CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N 6.2 (Medium) CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 【CVE-2026-114223】 6.7 (Medium) CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N 5.5 (Medium) CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
影響產品	NT OneAPP企業雲端管理系統 V1.5.22(含)以前版本
問題描述	【CVE-2026-114219(Hard-coded Credentials)】 未經身分鑑別之遠端攻擊者可取得硬編碼加密金鑰並解密登入請求內容，進而取得使用者明文帳號密碼及裝置資訊。 【CVE-2026-114220(Improper Certificate Validation)】 未經身分鑑別之鄰近網路攻擊者可利用應用程式未驗證伺服器憑證與主機名稱之缺陷進行中間人攻擊，進而攔截或竄改應用程式與伺服器間之通訊內容。 【CVE-2026-114221(Credential Disclosure)】 未經身分鑑別之遠端攻擊者可在特定條件下觸發WebView未驗證來源之HTTP Basic Authentication challenge，進而取得已登入使用者之NUP Portal通行碼。

	【CVE-2026-114222(Authentication Bypass)】 未經身分鑑別之本機端攻擊者可透過Deep Link繞過App PIN鎖定機制，進而存取已登入使用者之受保護資源。 【CVE-2026-114223(Exposure of Sensitive Information)】 未經身分鑑別之本機端攻擊者可在取得ADB備份存取授權並經使用者確認備份後，從備份資料中提取明文帳號通行碼，導致敏感資訊外洩。
解決方法	【CVE-2026-114219, CVE-2026-114220, CVE-2026-114223】 更新至NT OneAPP V1.5.35(含)以後版本 【CVE-2026-114221, CVE-2026-114222】 更新至 NT OneAPP V1.5.35(含)以後版本
公開日期	2026-10-22
相關連結	**https://www.twcert.org.tw/tw/cp-132-11307-ae4b3-1.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10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/**