TWCERT/CC 資安情資電子報

2026 年 4 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

勒索軟體組織「The Gentlemen」結合SystemBC惡意軟體擴大攻擊版圖

勒索軟體即服務（RaaS）組織「The Gentlemen」 自 2025 年中旬崛起後，近期透過整合 SystemBC 代理惡意軟體，使其攻擊規模於 2026 年第一季大幅擴張。該組織採取高度成熟的雙重勒索策略，不僅加密受害者的系統檔案，亦同步進行大規模關鍵商業資料外洩，以此作為威脅支付贖金的籌碼。近期，資安研究人員在事件回應調查中發現，The Gentlemen在入侵流程中大量部署「SystemBC」代理惡意軟體，經分析其C2伺服器資料後，揭露受害者數量已逾 1,570 名，主要分佈於美國、

英國及德國，感染特徵證實該攻擊具備高度針對性，精準鎖定企業與組織環境，而非一般個人使用者。

「SystemBC」是一款經常被利用於人為操作入侵流程中的代理惡意軟體。一旦於受害環境完成部署，該軟體即建立 SOCKS5 網路隧道，並透過自訂 RC4 加密協定連線至 C2 伺服器。此種加密代理通道不僅賦予攻擊者隱蔽通訊與橫向移動的能力，更整合了惡意酬載（Payload）的分發功能，可將後續程式碼直接寫入磁碟或注入記憶體中。在 The Gentlemen 的滲透活動中，SystemBC 常協同 Cobalt Strike 等後滲透工具，作為建立外部指令控制連線、分發勒索軟體、執行數據外傳及維持遠端持續存取的核心通道。

針對此對精密且具高度針對性的勒索軟體攻擊，企業應構件全面性的防護體系。首先，落實零信任架構（Zero Trust Architecture）為防範初期入侵的核心，包括嚴格禁止遠端桌面協定（RDP）直接暴露於公開網路、對所有管理介面實施強制性多重認證（MFA），並在 IT 管理工具與營運系統間執行嚴格的網路分段。在端點與安全強化方面，建議實施以下要點：

1. 端點防護強化：啟用防竄改與防漏洞利用攻擊功能，並以密碼保護資安軟體的解除安裝程序，藉此防止攻擊者在植入勒索軟體前，試圖停用關鍵的資安服務。
2. 定期修補系統漏洞：建立常態性的漏洞管理機制，優先修補VPN和防火牆等邊界設備之間關鍵漏洞。
3. 異常行為監測：持續監控環境內異常活動，特別是針對Active Directory (AD) 的大規模列舉查詢，或未經授權的遠端存取工具（如 AnyDesk、NetSupport）之安裝與連線。

4. 落實 3-2-1 備份策略：建立完善的檔案備份與還原機制，確保至少擁有3份備份，使用2種不同儲存媒體，並將其中1份存放於異地或採取離線隔離。

Check Point 研究團隊已針對 The Gentlemen 的攻擊行動發布相關入侵指標（IoC）如下：

描述	IoC
Cobalt Strike C&C	91.107.247[.]163
SystemBC	992c951f4af57ca7cd8396f5ed69c2199fd6fd4ae5e93726da3e198e78bec0a5
SystemBC C&C	45.86.230[.]112
The Gentlemen Windows	025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a 22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67 2ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d 3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235 48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd 62c2c24937d67fdeb43f2c9690ab10e8bb90713af46945048db9a94a465ffcb8 860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923 87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c 8c87134c1b45e990e9568f0a3899b0076f94be16d3c40fa824ac1e6c6ee892db 91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1 994d6d1edb57f945f4284cc0163ec998861c7496d85f6d45c08657c9727186e3 9f61ff4deb8afced8b1ecdc8787a134c63bde632b18293fbfc94a91749e3e454 a7a19cab7aab606f833fa8225bc94ec9570a6666660b02cc41a63fe39ea8b0ad b67958afc982cafbe1c3f114b444d7f4c91a88a3e7a86f89ab8795ac2110d1e6 c46b5a18ab3fb5fd1c5c8288a41c75bf0170c10b5e829af89370a12c86dd10f8 c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73 ec368ae0b4369b6ef0da244774995c819c63cffb7fd2132379963b9c1640ccd2 efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12 fc75ed2159e0c8274076e46a37671cfb8d677af9f586224da1713df89490a958
Embedded binaries (psexesvc.exe/psexec.exe)	cc14df781475ef0f3f2c441d03a622ea67cd86967526f8758ead6f45174db78e 078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b
gentlemen.bmp	fe1033335a045c696c900d435119d210361966e2fb5cd1ba3382608cfa2c8e68
The Gentlemen Linux	5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca 788ba200f776a188c248d6c2029f00b5d34be45d4444f7cb89ffe838c39b8b19 1eece1e1ba4b96e6c784729f0608ad2939cfb67bc4236dfababbe1d09268960c

- 相關連結
  1. SystemBC C2 Server Reveals 1,570+ Victims in The Gentlemen Ransomware Operation
  2. DFIR Report – The Gentlemen & SystemBC: A Sneak Peek Behind the Proxy
  3. Unmasking The Gentlemen Ransomware: Tactics, Techniques, and Procedures Revealed
  4. License to Encrypt: “The Gentlemen” Make Their Move

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 KrCERT/CC發布「Operation SearchStrike」報告：駭客以SEO毒化Github散布惡意軟體

韓國電腦網路危機處理暨協調中心（KrCERT/CC）的威脅狩獵分析團隊近期發布名為「Operation SearchStrike」報告。該報告指出，攻擊者正利用搜尋引擎最佳化中毒(SEO Poisoning） 技術，在搜尋引擎中推廣偽冒GitHub 儲存庫，藉此散布惡意軟體。此攻擊主要鎖定具備企業內部

高權限的技術人員，旨在以此作為跳板，進而發動全組織規模的橫向移動與滲透攻擊。

這波攻擊主要是透過 SEO Poisoning技術操弄搜尋排名，把內含惡意MSI安裝檔的假冒 GitHub 儲存庫推至搜尋結果首頁，常見偽冒程式像是Tftpd64、WinDbg、PsExec、Postman、USMT 這類網管與維運人員常用的工具，進行供應鏈層級的冒充攻擊，如圖1所示。一旦受害者誤下載並執行，系統會在背景植入以 Node.js 開發的惡意程式，並利用 Ethereum 智慧合約作為命令與控制(C2)通訊管道。由於採用去中心化機制，可降低對固定網域或 IP 的依賴，使傳統防火牆封鎖效果有限，進而增加偵測、阻擋與溯源的難度。

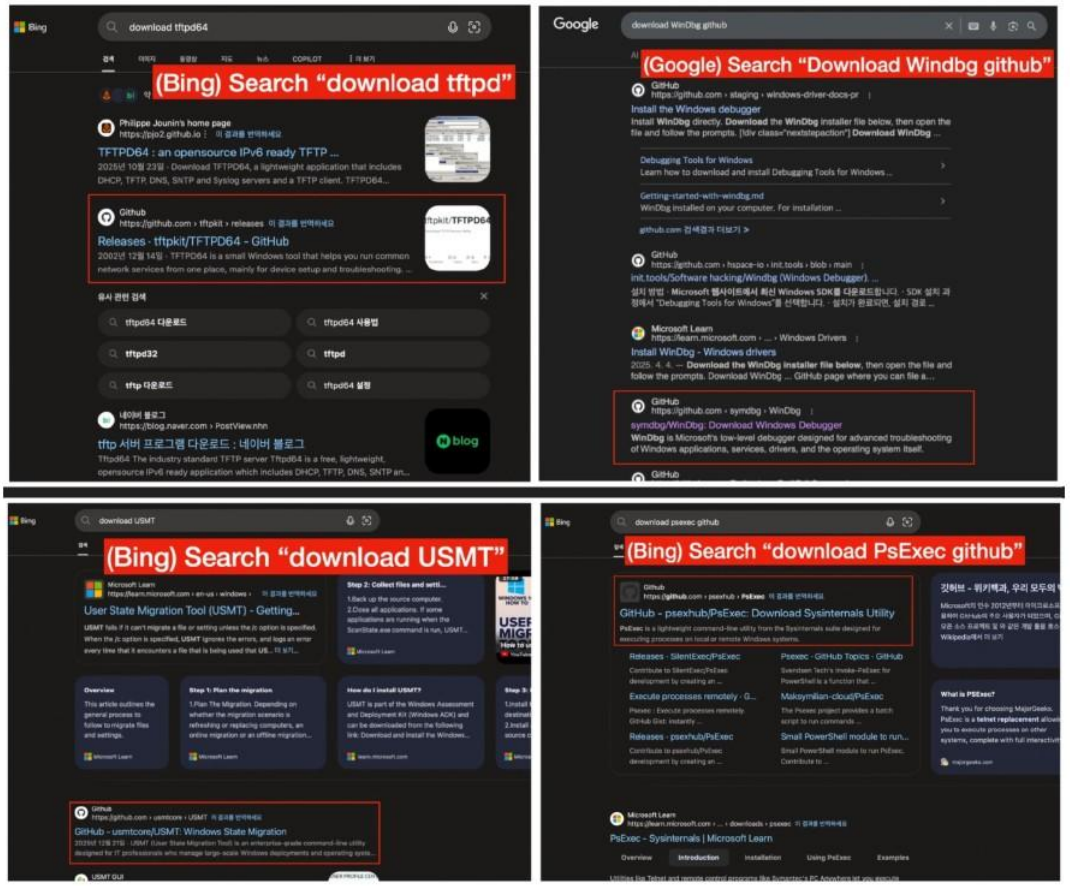

圖1：SEO Poisoning操控搜尋引擎排名。資料來源：KrCERT/CC

為防禦此類高隱蔽性的SEO攻擊，KrCERT/CC建議企業與技術人員採取以下防禦策略：

1. 強化供應鏈來源控管：企業應嚴格限制軟體下載途徑，確保僅透過Microsoft Store、官方網站或經官方認證的 GitHub 儲存庫取得工具。針對 GitHub 專案，使用者於下載前必須執行「盡職調查（Due Diligence）」，仔細辨識儲存庫的星號（Stars）數量、貢獻者歷史紀錄（Contributors）及帳號建立日期，以排除近期建立且缺乏社群信任基礎的偽造專案。
2. 落實入侵指標（IoC）清查：企業資安團隊可參照報告提供的IoC，針對權組織端點進行深度掃描，清查重點包含檔案雜湊值（Hash）、異常路徑、針對區塊鏈節點的異常請求等。
3. 疑似感染應變程序：若於內部環境偵測到疑似感染跡象，應立即啟動資安應變機制，優先隔離受影響主機以防止攻擊者進一步橫向攻擊，並針對受影響帳號進行憑證重設與權限審核，防堵潛在的擴散風險。

KrCERT/CC針對此次攻擊提供入侵指標（IoC）如下：

建立時間	偽冒軟體	SHA256
2026-02-17	Tftpd64	d6acbd0cf0c99c76c3f09f68792eabb843fd539ae42573ecdfeda63fa695dcd2
2026-02-17	Postman	3ddfcc93aefab5a671edb4c643a810b7a2a7b35629c27f3f68849cf390a26025
2026-02-23	Tftpd64	c3910810dc87e1a5993d4e4234fd3f94fa7ecf66735fd0396be73b2379aafabd
2026-03-09	Tftpd64	3abe9aa1b6a9f2f779f875773e077e0129e770e98fcbee60c0137f656f4fe82e
2026-03-10	Tftpd64	ece54f2a68530222604014dd5b23520bb1729efe7ea15a822c1ea16556ed8257
2026-03-10	WinDbg	ab79d9ef9fddb880bbfc5e2587566884da9510988005f2737493cfc25437b8ba

2026-03-10	PsExec	c03e9aade86079a2d4007b58e3b419dfe821bf64366fd3a9c3d04dd63b5e7779
2026-03-10	USMT	eb2a4c6e88adc5b56dcb6a39bf749564d5b72fbb5ba2dc3c603ba183a99bccb4
2026-03-10	IntuneWinAppUtil	fc9da1e9c12930f1c324b4dee5918033a644d090a96f69ff3669711d4219158b
2026-03-10	BgInfo	e3df11e259647e00de5f6119fce20c07f551b4bb5b3c4da3fb07956c0c3d69ff
2026-03-10	RDCMan	f88532089976d65463869a1ab5e8f050d8f3ee49501a5fa7883f80ac86b20a84

C2 Domain：

jariosos[.]com

hayesmed[.]com

regancontrols[.]com

salinasrent[.]com

justtalken[.]com

mebeliotmasiv[.]com

euclidrent[.]com

o-parana[.]com

palshona[.]com

aurineuroth[.]com

- 相關連結

1. Operation SearchStrike

2.2 軟硬體系統資安議題

2.2.1 UAT-10608大規模自動化竊密行動：鎖定React2Shell漏洞入侵逾700台Next.js伺服器

思科旗下資安威脅情報與研究團隊 Cisco Talos 近日揭露，一個被追蹤為「UAT-10608」的威脅叢集，正針對暴露於網路的Next.js應用程式發動大規模自動化憑證竊取行動。該組織利用去年底備受關注的 React2Shell 漏洞（CVE-2025-55182），結合名為「NEXUS Listener」的自動化資料蒐集框架，在短時間內入侵全球至少766台主機，影響範圍橫跨多個地區與雲端服務供應商。

React2Shell（CVE-2025-55182）為一項高風險 RCE 漏洞，允許未經

驗證的遠端攻擊者，在缺乏適當輸入驗證和處理的應用程式環境中執行任意程式碼，影響 React 與 Next.js 等主流前端框架。報告指出，UAT-10608 的攻擊具高度系統化特徵，先透過 Shodan、Censys 或自訂掃描器大規模探測暴露於公開網路的 Next.js環境；確認存在漏洞後，即向 Server Function 端點發送惡意序列化酬載，於伺服器端 Node.js 程序中執行任意程式碼。

取得初始存取權限後，攻擊者會在系統 /tmp 目錄下植入隨機命名的 Shell 指令碼，並透過 nohup 指令執行，展開自動化資料蒐集。竊取內容涵蓋帳號憑證（如 SSH 金鑰與各類存取令牌）、雲端與容器環境資訊（如 Kubernetes 與雲端 metadata）、系統環境參數（如環境變數），以及操作歷史與程序執行資訊等敏感資料。

外洩資料會回傳至C2基礎設施並儲存於資料庫中，並透過名為「NEXUS Listener」的網頁應用程式存取。研究人員指出，該框架具備完善的圖形化介面（GUI）與分析儀表板，可即時統計受害主機數量、憑證類型與系統運行狀態，並提供搜尋功能，協助攻擊者從大量資料中篩選高價值目標，進一步發動供應鏈攻擊或轉售存取權限。

面對 UAT-10608 的攻擊行動，Cisco Talos建議企業採取以下防禦措施：

- **優先修補漏洞：**立即修補 Next.js 環境中的 CVE-2025-55182。
- **全面輪替憑證：**若疑似遭入侵，應輪換所有可能外洩的憑證與API金鑰，並避免SSH 金鑰跨系統重複使用。
- **強化雲端與架構安全：**於 AWS EC2 啟用 IMDSv2 ，降低中繼資料服務遭濫用風險；同時盤點容器權限，避免過度授權或存取主機 SSH 代理。

- **程式碼檢視：**檢查 getServerSideProps 與 getStaticProps 實作，避免敏感資料外洩，並審慎使用 NEXT_PUBLIC_ 前綴。
- **監控入侵指標（IoC）：**留意 /tmp/ 目錄中異常檔案、不尋常的 nohup 執行紀錄，以及應用程式異常對外 HTTP/S 連線。

- 相關連結

1. UAT-10608: Inside a large-scale automated credential harvesting operation targeting web applications
2. Automated Credential Harvesting Campaign Exploits React2Shell Flaw
3. Hackers exploit React2Shell in automated credential theft campaign
4. Cisco-Talos/IOCs

2.3 軟硬體漏洞資訊

2.3.1 Internet Systems Consortium (ISC) 的BIND存在重大資安漏洞(CVE-2026-3104)

CVE 編號	CVE-2026-3104
影響產品	BIND
解決辦法	根據官方網站釋出的解決方式進行修補： https://kb.isc.org/docs/cve-2026-3104

- 內容說明：

  近日 Internet Systems Consortium (ISC)針對 BIND 發布重大資安公告(CVE-2026-3104，CVSS：7.5)，此漏洞可透過精心設計的域名，造成 BIND 解析器中記憶體洩漏。

- 影響平台：
  - BIND 9.20.0 至 9.20.20 版本
  - BIND 9.21.0 至 9.21.19 版本
  - BIND 9.20.9-S1 至 9.20.20-S1 版本
- 資料來源：
  1. CVE-2026-3104: Memory leak in code preparing DNSSEC proofs of non-existence
  2. CVE-2026-3104

2.3.2 FortiClientEMS存在重大資安漏洞(CVE-2026-35616)

CVE 編號	CVE-2026-35616
影響產品	FortiClientEMS
解決辦法	請更新至 FortiClientEMS 7.4.7(含)之後版本

- 內容說明：

  FortiClientEMS 是 Fortinet 旗下一款端點管理伺服器，用於集中管理 FortiClient 代理程式，支持端點部署、設定與監控。近日發布重大資安漏洞公告(CVE-2026-35616，CVSS：9.8)，此為不當存取控制漏洞，可能允許未經身分驗證的攻擊者，透過精心建構的請求執行未經授權的程式碼或命令。

- 影響平台：
  - FortiClientEMS 7.4.5 至 7.4.6(含)版本
- 資料來源：
  1. API authentication and authorization bypass
  2. CVE-2026-35616

2.3.3 Cisco旗下Smart Software Manager(本機部署版)存在重大資安漏洞(CVE-2026-20160)

CVE 編號	CVE-2026-20160
影響產品	Cisco Smart Software Manager On-Prem
解決辦法	請更新至 Cisco Smart Software Manager On-Prem 9-202601 (含)之後版本

- 內容說明：

  近日 Cisco 針對 Smart Software Manager 發布重大資安公告(CVE-2026-20160，CVSS：9.8)，該漏洞可能允許未經身分驗證的遠端攻擊者於底層作業系統上執行任意命令。

- 影響平台：
  - Cisco Smart Software Manager On-Prem 9-202502 至 9-202510 版本
- 資料來源：
  1. Cisco Smart Software Manager On-Prem Arbitrary Command Execution Vulnerability
  2. CVE-2026-20160

2.3.4 Cisco旗下Integrated Management Controller 存在2個重大資安漏洞

CVE 編號	CVE-2026-20093,CVE-2026-20094
影響產品	Cisco Integrated Management Controller
解決辦法	根據官方網站釋出的解決方式進行修補： 【CVE-2026-20093】 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn 【CVE-2026-20094】 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt

- 內容說明：

  Cisco 旗下整合管理控制器(Integrated Management Controller，IMC)是一款專門為 Cisco 整合運算系統的伺服器設計管理工具，提供伺服器遠端監控、配置和管理功能，近日 Cisco 發布重大資安公告(CVE-2026-20093，CVSS：9.8 和 CVE-2026-20094，CVSS：8.8)。CVE-2026-20093 為身分驗證繞過漏洞，可能允許未經身分驗證的遠端攻擊者繞過身分驗證，並以管理員身分存取系統；CVE-2026-20094 存在於 IMC 的 Web 管理介面，此為命令注入漏洞，經身分驗證的遠端攻擊者可能在受影響的底層作業系統上，執行任意程式碼或命令，並將權限提升至 root。

- 影響平台：

  【CVE-2026-20093】

  - Cisco 5000 Series ENCS 4.15(含)之前版本
  - Cisco Catalyst 8300 Series Edge uCPE 4.16(含)之前版本
  - Cisco Catalyst 8300 Series Edge uCPE 4.18 版本
  - UCS C-Series M5 Rack Server 4.2(含)之前版本

- UCS C-Series M5 Rack Server 4.3 版本
- UCS C-Series M6 Rack Server 4.2(含)之前版本
- UCS C-Series M6 Rack Server 4.3
- UCS C-Series M6 Rack Server 6.0
- UCS E-Series M3 3.2 (含)之前版本
- UCS E-Series M6 4.15 (含)之前版本

【CVE-2026-20094】

- Cisco Catalyst 8300 Series Edge uCPE 4.16(含)之前版本
- Cisco Catalyst 8300 Series Edge uCPE 4.18 版本
- UCS C-Series M5 Rack Server 4.2(含)之前版本
- UCS C-Series M5 Rack Server 4.3 版本
- UCS C-Series M6 Rack Server 4.2(含)之前版本
- UCS C-Series M6 Rack Server 4.3
- UCS C-Series M6 Rack Server 6.0
- UCS E-Series M6 4.15 (含)之前版本
- UCS S-Series Storage Server 4.2(含)之前版本
- UCS S-Series Storage Server 4.3

- 資料來源：
  1. Cisco Integrated Management Controller Authentication Bypass Vulnerability
  2. Cisco Integrated Management Controller Command Injection and Remote Code Execution Vulnerabilities
  3. CVE-2026-20093
  4. CVE-2026-20094

2.3.5 GNU Inetutils Telnetd存在重大資安漏洞(CVE-2026-32746)

CVE 編號	CVE-2026-32746
影響產品	GNU Inetutils Telnetd
解決辦法	建議停用 Telnet 服務，並於修補程式釋出後儘速更新；如無法停用，應限制存取以降低風險。

- 內容說明：

  研究人員發現 GNU Inetutils Telnetd 存在緩衝區溢位(Buffer Overflow)漏洞(CVE-2026-32746，CVSS：9.8)，未經身分驗證的遠端攻擊者可利用此漏洞執行任意程式碼，請儘速確認並進行修補。

- 影響平台：
  - GNU Inetutils Telnetd 2.7(含)以前版本
- 資料來源：
  1. CVE-2026-32746

2.3.6 Junos OS MX 系列存在重大資安漏洞(CVE-2026-33785)

CVE 編號	CVE-2026-33785
影響產品	Junos OS MX
解決辦法	請更新至 Junos OS MX 系列 24.4R2-S3、25.2R2、25.4R1 (含)之後版本

- 內容說明：

  Juniper Networks Junos OS MX 系列交換器的 CLI 存在重大資安漏洞(CVE-2026-33785，CVSS：8.8)，此漏洞為允許已驗證之低權限使用者執行未授權之高權限指令，可能導致設備遭未授權控制。

- 影響平台：
  - Junos OS MX 系列 24.4R2-S3 版本(不含)之前版本
  - Junos OS MX 系列 25.2R2 版本
- 資料來源：
  1. 2026-04 Security Bulletin: Junos OS: MX Series (CVE-2026-33785)

2.3.7 Juniper Networks Support Insights vLWC存在重大資安漏洞(CVE-2026-33784)

CVE 編號	CVE-2026-33784
影響產品	Juniper Networks Support Insights vLWC
解決辦法	請更新至 Juniper Networks Support Insights vLWC 3.0.94 (含)之後版本

- 內容說明：
  Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC) 存在重大資安漏洞(CVE-2026-33784，CVSS：9.8)，此為使用預設密碼漏洞，允許攻擊者使用已知預設憑證登入並取得高權限存取，進而可能控制設備。
- 影響平台：
  - Juniper Networks Support Insights vLWC 3.0.94 (不含)之前版本
- 資料來源：
  1. 2026-04 Security Bulletin: vLWC (CVE-2026-33784)

2.3.8 Juniper Networks CTP OS 存在重大資安漏洞(CVE-2026-33771)

CVE 編號	CVE-2026-33771
影響產品	Juniper Networks CTP OS
解決辦法	請更新至 Juniper Networks CTP OS 9.3R1(含)之後版本

- 內容說明：

  Juniper Networks CTP OS 存在重大資安漏洞(CVE-2026-33771，CVSS 4.x：9.1)，此為弱密碼要求漏洞，可能允許未經身分驗證的網路攻擊者，利用本機帳號的弱密碼取得設備控制權。

- 影響平台：
  - Juniper Networks CTP OS 9.2R1 和 9.2R2 版本
- 資料來源：
  1. 2026-04 Security Bulletin: CTP OS (CVE-2026-33771)

2.3.9 Palo Alto Cortex XSIAM / XSOAR 存在重大資安漏洞(CVE-2026-0234)

CVE 編號	CVE-2026-0234
影響產品	Palo Alto Cortex XSIAM / XSOAR
解決辦法	請更新至以下版本： Cortex XSIAM Microsoft Teams Marketplace 1.5.52(含)之後版本 Cortex XSOAR Microsoft Teams Marketplace 1.5.52(含)之後版本

- 內容說明：

  近日 Palo Alto Networks 發布重大資安公告(CVE-2026-0234，CVSS：7.2)，Cortex XSOAR 和 Cortex XSIAM 平台整合 Microsoft Teams 時，存在加密簽章不當漏洞，允許未經身分驗證的攻擊者存取或竄改受保護的資源。

- 影響平台：
  - Cortex XSIAM Microsoft Teams Marketplace 1.5.52 (不含)之前版本
  - Cortex XSOAR Microsoft Teams Marketplace 1.5.52 (不含)之前版本
- 資料來源：
  1. CVE-2026-0234 Cortex XSOAR

2.3.10 Fortinet 旗下 FortiSandbox 存在重大資安漏洞(CVE-2026-39808)

CVE 編號	CVE-2026-39808
影響產品	FortiSandbox
解決辦法	請更新至 FortiSandbox 4.4.9 (含)之後版本

- 內容說明：

  FortiSandbox 是 Fortinet 旗下一款威脅防護解決方案，可執行動態分析以識別先前未知的網路威脅。Fortinet 發布 FortiSandbox 存在重大資安漏洞(CVE-2026-39808，CVSS：9.8)，此為作業系統指令注入漏洞，可允許未經過身分驗證的攻擊者，透過特製的 HTTP 請求執行未經授權的程式碼或指令。

- 影響平台：
  - FortiSandbox 4.4.0 至 4.4.8(含)版本
- 資料來源：
  1. OS Command Injection through API endpoint
  2. CVE-2026-39808

2.3.11 Fortinet 旗下 FortiSandbox JRPC API 存在重大資安漏洞(CVE-2026-39813)

CVE 編號	CVE-2026-39813
影響產品	FortiSandbox
解決辦法	請更新至以下版本： FortiSandbox 4.4.9 (含)之後版本 FortiSandbox 5.0.6 (含)之後版本

- 內容說明：

  Fortinet 發布 FortiSandbox JRPC API 存在重大資安漏洞(CVE-2026-39813，CVSS：9.8)，此為路徑遍歷漏洞，可能允許未經過身分驗證的攻擊者，透過特製的 HTTP 請求繞過身分驗證。

- 影響平台：
  - FortiSandbox 4.4.0 至 4.4.8 (含)版本
  - FortiSandbox 5.0.0 至 5.0.5 (含)版本
- 資料來源：
  1. Unauthenticated Authentication bypass and Privilege escalation in FortiSandbox
  2. CVE-2026-39813

2.3.12 SAP 商業規畫與合併財務報表系統和企業資料倉儲系統存在重大資安漏洞 (CVE-2026-27681)

CVE 編號	CVE-2026-27681
影響產品	SAP Business Planning and Consolidation、Business Warehouse
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/april-2026.html

- 內容說明：

  SAP 針對旗下產品商業規畫與合併財務報表系統(SAP Business Planning and Consolidation)和企業資料倉儲系統(SAP Business Warehouse)發布重大資安漏洞公告(CVE-2026-27681，CVSS：9.9)，允許經身分驗證的攻擊者，透過特製的 SQL 語法讀取、修改和刪除資料庫資料，對系統的機密性、完整性和可用性造成影響。

- 影響平台：
  - HANABPC 810, BPC4HANA 300, SAP_BW 750, 752, 753, 754, 755, 756, 757, 758, 816
- 資料來源：
  1. SAP Security Patch Day - April 2026
  2. CVE-2026-27681

2.3.13 Cisco 旗下身分識別服務存在3個重大資安漏洞

CVE 編號	CVE-2026-20180,CVE-2026-20186,CVE-2026-20147
影響產品	Cisco ISE
解決辦法	請更新至以下版本： 【CVE-2026-20180、CVE-2026-20186】 Cisco ISE 3.2 Patch 8 Cisco ISE 3.3 Patch 8 Cisco ISE 3.4 Patch 5 【CVE-2026-20147】 Cisco ISE 或 Cisco ISE-PIC 3.1 Patch 11 Cisco ISE 或 Cisco ISE-PIC 3.2 Patch 10 Cisco ISE 或 Cisco ISE-PIC 3.3 Patch 11 Cisco ISE 或 Cisco ISE-PIC 3.4 Patch 6 Cisco ISE 或 Cisco ISE-PIC 3.5 Patch 3 備註：Cisco ISE-PIC 已停止販售，3.4 版本是最後一個支援的版本

- 內容說明：

  Cisco 旗下身分識別服務引擎(Identity Services Engine，ISE)是一款基於身分的安全管理平台，可從網路、使用者設備收集資訊，並在網路基礎設施中實施策略和制定監管決策，近日 Cisco 發布重大資安漏洞公告。

  【CVE-2026-20180，CVSS：9.9 和 CVE-2026-20186，CVSS：9.9】皆為遠端執行程式碼漏洞，允許經身分驗證的遠端攻擊者，可在受影響的底層作業系統上執行任意命令。若利用該漏洞，成功利用此漏洞的前提為攻擊者至少具備唯讀管理者權限。

【CVE-2026-20147，CVSS：9.9】

此漏洞允許經身分驗證的遠端攻擊者在受影響設備的底層作業系統上執行任意命令，成功利用此漏洞的前提為攻擊者至少擁有有效的管理員憑證。

- 影響平台：

【CVE-2026-20180、CVE-2026-20186】

- Cisco ISE 3.2(含)之前版本
- Cisco ISE 3.2、3.3、3.4 版本

【CVE-2026-20147】

- Cisco ISE 或 Cisco ISE-PIC 3.1(含)之前版本
- Cisco ISE 或 Cisco ISE-PIC 3.2、3.3、3.4、3.5 版本

備註：Cisco ISE-PIC 已停止販售，3.4 版本是最後一個支援的版本

- 資料來源：

1. Cisco Identity Services Engine Remote Code Execution Vulnerabilities
2. Cisco Identity Services Engine Remote Code Execution and Path Traversal Vulnerabilities
3. CVE-2026-20180
4. CVE-2026-20186
5. CVE-2026-20147

2.3.14 Cisco Webex Services 存在重大資安漏洞(CVE-2026-20184)

CVE 編號	CVE-2026-20184
影響產品	Cisco Webex Services
解決辦法	根據官方網站釋出的解決方式進行修補： https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cui-cert-8jSZYhWL

- 內容說明：

  近日 Cisco 發布重大資安漏洞公告(CVE-2026-20184，CVSS：9.8)，此漏洞源於憑證驗證不當，在 Cisco Webex Services 單一登入(SSO)與 Control Hub 整合過程中，可能允許未經身分驗證的遠端攻擊者冒充服務中的任意使用者。

- 影響平台：
  - 當 Cisco Webex Services 設定透過 SSO 與 Control Hub 整合過程
- 資料來源：
  1. Cisco Webex Services Certificate Validation Vulnerability
  2. CVE-2026-20184

2.3.15 Microsoft SQL Server 存在重大資安漏洞(CVE-2026-33120)

CVE 編號	CVE-2026-33120
影響產品	Microsoft SQL Server
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/en-US/vulnerability/CVE-2026-33120

- 內容說明：

  微軟針對旗下產品 SQL Server 發布重大資安漏洞公告(CVE-2026-33120，CVSS：8.8)，此為 Untrusted Pointer Dereference 漏洞，允許授權的攻擊者透過網路執行程式碼。

- 影響平台：
  - Microsoft SQL Server 2022 (GDR) 16.0.0 至 16.0.1175.1(不含)版本
- 資料來源：
  1. Microsoft SQL Server Remote Code Execution Vulnerability
  2. CVE-2026-33120

2.3.16 Windows Desktop 遠端桌面客戶端存在重大資安漏洞(CVE-2026-32157)

CVE 編號	CVE-2026-32157
影響產品	Windows Desktop
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/en-US/vulnerability/CVE-2026-32157

- 內容說明：

  微軟針對旗下產品 Windows Desktop 遠端桌面客戶端發布重大資安漏洞公告(CVE-2026-32157，CVSS：8.8)，此漏洞允許未經授權的攻擊者透過網路執行程式碼。

- 影響平台：
  - Windows Desktop 遠端桌面客戶端 1.2.0.0 至 2.0.1070.0 版本
- 資料來源：
  1. Remote Desktop Client Remote Code Execution Vulnerability
  2. CVE-2026-32157

2.3.17 Adobe Acrobat Reader存在高風險安全漏洞(CVE-2026-34621)

CVE 編號	CVE-2026-34621
影響產品	Adobe Acrobat Reader
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://helpx.adobe.com/security/products/acrobat/apsb26-43.html

- 內容說明：

  研究人員發現 Adobe Acrobat Reader 存在原型鏈汙染(Prototype Pollution)漏洞(CVE-2026-34621，CVSS：8.6)，未經身分鑑別之攻擊者可誘使使用者開啟特製惡意檔案，污染程式執行時之物件原型，進而於目前使用者權限執行任意程式碼。此漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - Acrobat DC Continuous 26.001.21367(含)以前版本
  - Acrobat Reader DC Continuous 26.001.21367(含)以前版本
  - Adobe Acrobat 2024 Classic 24.001.30356(含)以前版本
- 資料來源：
  1. Security update available for Adobe Acrobat Reader | APSB26-43
  2. CVE-2026-34621

2.3.18 Apache ActiveMQ Classic存在高風險安全漏洞(CVE-2026-34197)

CVE 編號	CVE-2026-34197
影響產品	Apache ActiveMQ Classic
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://activemq.apache.org/security-advisories.data/CVE-2026-34197-announcement.txt

- 內容說明：

  研究人員發現 Apache ActiveMQ Classic 存在不當輸入驗證(Improper Input Validation)與程式碼注入(Code Injection)漏洞(CVE-2026-34197，CVSS：8.8)，因 Web Console 暴露之 Jolokia JMX-HTTP 介面允許執行特定操作且缺乏輸入驗證，使已通過身分鑑別之遠端攻擊者可傳入惡意參數，進而執行任意程式碼。此漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - Apache ActiveMQ Broker 5.19.4(不含)以前版本
  - Apache ActiveMQ Broker 6.0.0 至 6.2.3(不含)版本
  - Apache ActiveMQ 5.19.4(不含)以前版本
  - Apache ActiveMQ 6.0.0 至 6.2.3(不含)版本
- 資料來源：
  1. Severity: important
  2. CVE-2026-34197

第 3 章、資安研討會及活動

- **資安研討會**

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

【工作坊】5/21-台北場-資服業者個資交流工作坊(限資服業者)	
活動時間	**2026-05-21 13:30 ~ 2026-05-21 16:30**
活動地點	**DigiBlock C數位創新基地 (臺北市大同區承德路三段287號C棟)**
活動網站	**https://www.tissa.org.tw/Course/Detail/5977**
活動概要	 **【費用】** 免費 報名截止： 2026-05-18 **【活動內容 / Event Deails】** 別等稽查上門，您的個資保護落實了嗎？ 本場交流工作坊，特邀法律與資安專家帶領您拆解個資法遵重點，手把手解析「個資安全維護計畫」撰寫架構與常見疑義。下半場活

	動採分組討論進行，讓您與專家一對一提問、即時回饋，釐清制度建置卡關處，帶回可立即運用的具體做法，讓法遵不再只是紙上談兵。 限定資服業者報名，名額有限，敬請提早報名，避免向隅。 **【主辦單位】數位發展部數位產業署** **【執行單位】財團法人資訊工業策進會、中華民國資訊軟體協會** **【聯絡窗口】02-2553-3988#816 林專員** **security@tissa.org.tw**
115年個人資料檔案安全維護計畫一對一線上健檢諮詢(限定資訊服務業者參與)	
活動時間	**2026-03-25 13:30 ~ 2026-07-30 14:30**
活動地點	**採預約制，線上Teams會議室**
活動網站	**https://www.tissa.org.tw/Course/Detail/5976**
活動概要	 **【費用】** 免費 報名截止： 2026-07-30 **【活動內容 / Event Deails】** 個資保護不只合規，專家一對一陪你實務到位！貴公司的個資安全維護計畫，經得起檢查嗎？小心受罰 2 萬元以上 200 萬元以下罰

	緩！本活動由法律 + 資安專家團隊協助資服業者 1 on 1 線上諮詢。不僅協助快速找出關鍵漏洞，更提供最貼近實務面的改善建議作法！限 50 家資訊服務業者參與，立即搶先報名！ *請在報名頁面【備註】欄位，留下三個您方便的日期，承辦人將收到您的資訊後，安排一對一線上健檢諮詢時段，謝謝！ **【主辦單位】財團法人資訊工業策進會** **【執行單位】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：

達煬科技｜WinMatrix - Missing Authentication	
TVN / CVE ID	TVN-202604001 / CVE-2026-6348
CVSS	8.8 (High) CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
影響產品	WinMatrix agent程式 3.5.13至3.5.26.15版本
問題描述	達煬科技開發之WinMatrix agent程式存在Missing Authentication漏洞，已通過身分鑑別之本機端攻擊者可於本機與該環境內所有安裝agent程式之主機上以系統權限執行任意程式碼。
解決方法	請更新agent程式至3.5.27.5(含)以後版本
公開日期	2026-04-16
相關連結	https://www.twcert.org.tw/tw/cp-132-10839-2d9a7-1.html
桓基科技｜iSherlock - OS Command Injection	
TVN / CVE ID	TVN-202604002 / CVE-2026-6349
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	影響產品： Hgiga iSherlock 4.5與5.5(包含 MailSherlock、SpamSherlock、AuditSherlock) 影響套件： iSherlock-base-4.5 476(不含)以前版本 iSherlock-audit-4.5 261(不含)以前版本 iSherlock-base-5.5 476(不含)以前版本

	iSherlock-audit-5.5 261(不含)以前版本
問題描述	桓基科技開發之iSherlock存在OS Command Injection漏洞，未經身分鑑別之本機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	更新iSherlock-base-4.5套件至476(含)以後版本 更新iSherlock-audit-4.5套件至261(含)以後版本 更新iSherlock-base-5.5套件至476(含)以後版本 更新iSherlock-audit-5.5套件至261(含)以後版本
公開日期	2026-04-16
相關連結	**https://www.twcert.org.tw/tw/cp-132-10842-3f255-1.html**
網擎資訊｜MailGates/MailAudit - Stack-based Buffer Overflow	
TVN / CVE ID	TVN-202604003 / CVE-2026-6350
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	MailGates/MailAudit 6.0： 6.1.10.054(不含)以前版本 MailGates/MailAudit 5.0： 5.2.10.099(不含)以前版本
問題描述	CVE-2026-6350(Stack-based Buffer Overflow)： 未經身分鑑別之遠端攻擊者可控制程式執行流程並執行任意程式碼。
解決方法	MailGates/MailAudit 6.0： Update to version 6.1.10.054 or later MailGates/MailAudit 5.0： Update to version 5.2.10.099 or later
公開日期	2026-04-16
相關連結	**https://www.twcert.org.tw/tw/cp-132-10844-1405d-1.html**
鼎新數智｜EasyFlow.NET - 存在2個漏洞	

TVN / CVE ID	TVN-202604006 / CVE-2026-5963, CVE-2026-5964
CVSS	【CVE-2026-5963】 9.8(Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 【CVE-2026-5964】 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	【CVE-2026-5963】 EasyFlow .NET V6.1.x, V6.6.x, V8.1.1, V8.1.2, V8.1.3, V8.1.4 【CVE-2026-5964】 EasyFlow .NET V6.1.x, V6.6.x, V8.1.1, V8.1.2
問題描述	【CVE-2026-5963(SQL Injection)】 未經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。 【CVE-2026-5964(SQL Injection)： 未經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	【CVE-2026-5963】 更新至 v8.1.5(含)以後版本或執行Patch更新至 2026/01/20 的版本 【CVE-2026-5964】 更新至 v8.1.3(含)以後版本或執行Patch更新至 2026/01/20 的版本
公開日期	2026-04-20
相關連結	https://www.twcert.org.tw/tw/cp-132-10831-a734d-1.html

TVN / CVE ID	TVN-202604007 / CVE-2026-5967
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	ThreatSonar Anti-Ransomware 4.0.0(不含)以前版本
問題描述	【CVE-2026-5967(Privilege Escalation)】 已通過身分鑑別且具shell操作權限之遠端攻擊者可注入作業系統指令並以root權限執行。
解決方法	請安裝修補程式20260302版本
公開日期	2026-04-20
相關連結	**https://www.twcert.org.tw/tw/cp-132-10854-03015-1.html**
力新國際｜NewSoftOA - OS Command Injection	
TVN / CVE ID	TVN-202604008 / CVE-2026-5965
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	NewSoftOA 10.1.8.3(不含)以前版本
問題描述	力新國際開發之NewSoftOA存在OS Command Injection漏洞，未經身分鑑別之本機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	更新至10.1.8.3(含)以後版本
公開日期	2026-04-21
相關連結	**https://www.twcert.org.tw/tw/cp-132-10856-4979f-1.html**
博格科技｜Borg SPM 2007 - 存在3個漏洞	
TVN / CVE ID	TVN-202604009 / CVE-2026-6885, CVE-2026-6886, CVE-2026-6887
CVSS	【CVE-2026-6885】 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

	【CVE-2026-6886】 9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 【CVE-2026-6887】 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	Borg SPM 2007(於2008年停售)
問題描述	【CVE-2026-6885(Arbitrary File Upload)】 未經身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼。 【CVE-2026-6886(Authentication Bypass)】 未經身分鑑別之遠端攻擊者可以任意使用者登入系統。 【CVE-2026-6887(SQL Injection)】 未經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	無論系統版本為何，凡有持續簽署維護合約之客戶，請聯繫廠商協助進行修補，或升級至最新版本系統(SPM2025 SP1已通過原碼檢測)。 若未簽署維護合約且仍持續使用該版本系統之用戶，請聯繫廠商以討論後續處理事宜。
公開日期	2026-04-23
相關連結	**https://www.twcert.org.tw/tw/cp-132-10861-b8709-1.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4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/**