張貼日期：2025/05/07

【漏洞預警】CISA新增8個已知遭駭客利用之漏洞至KEV目錄(2025/04/28-2025/05/04)

- 主旨說明:【漏洞預警】CISA新增8個已知遭駭客利用之漏洞至KEV目錄(2025/04/28-2025/05/04)
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202505-00000002】

1. 【CVE-2025-1976】Broadcom Brocade Fabric OS Code Injection Vulnerability (CVSS v3.1: 6.7)
   【是否遭勒索軟體利用:未知】 Broadcom Brocade Fabric OS存在程式碼注入漏洞，該漏洞允許具有管理權限的本機使用者以完整的root權限執行任意程式碼。
   【影響平台】請參考官方所列的影響版本
   https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25602
2. 【CVE-2025-42599】Qualitia Active Mail Stack-Based Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
   【是否遭勒索軟體利用:未知】 Qualitia Active Mail存在堆疊緩衝區溢位漏洞，該漏洞允許遠端未經驗證的攻擊者透過特製的請求執行任意程式碼或觸發DoS攻擊。
   【影響平台】請參考官方所列的影響版本
   https://www.qualitia.com/jp/news/2025/04/18_1030.html
3. 【CVE-2025-3928】Commvault Web Server Unspecified Vulnerability (CVSS v3.1: 8.8)
   【是否遭勒索軟體利用:未知】 Commvault Web Server存在安全性漏洞，該漏洞允許遠端經驗證的攻擊者建立並執行 Web Shell】
   【影響平台】請參考官方所列的影響版本
   https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html
4. 【CVE-2025-31324】SAP NetWeaver Unrestricted File Upload Vulnerability (CVSS v3.1: 9.8)
   【是否遭勒索軟體利用:未知】 SAP NetWeaver Visual Composer Metadata Uploader存在不受限制的檔案上傳漏洞，該漏洞允許未經驗證的攻擊者上傳可能具有惡意的可執行二進位檔案。
   【影響平台】 SAP NetWeaver 7.5
5. 【CVE-2024-38475】Apache HTTP Server Improper Escaping of Output Vulnerability (CVSS v3.1: 9.1)
   【是否遭勒索軟體利用:未知】 Apache HTTP Server在mod rewrite中存在不當逃逸輸出漏洞，該漏洞允許攻擊者將 URL映射到伺服器允許提供但原本不應被直接或有意存取的檔案系統位置，可能導致程式碼執行或原始碼洩漏。
   【影響平台】請參考官方所列的影響版本
   https://httpd.apache.org/security/vulnerabilities_24.html
6. 【CVE-2023-44221】SonicWall SMA100 Appliances OS Command Injection Vulnerability (CVSS v3.1: 7.2)
   【是否遭勒索軟體利用:未知】 SonicWall SMA100裝置的SSL-VPN管理介面存在作業系統指令注入漏洞，該漏洞允許具備管理權限的遠端已驗證攻擊者以【nobody】使用者身份注入任意指令。
   【影響平台】請參考官方所列的影響版本
   https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018
7. 【CVE-2025-34028】Commvault Command Center Path Traversal Vulnerability (CVSS v3.1: 10.0)
   【是否遭勒索軟體利用:未知】 Commvault Command Center存在路徑遍歷漏洞，該漏洞允許遠端未經驗證的攻擊者執行任意程式碼。
   【影響平台】請參考官方所列的影響版本
   https://documentation.commvault.com/securityadvisories/CV_2025_04_1.html

8. □CVE-2024-58136□Yiiframework Yii Improper Protection of Alternate Path Vulnerability (CVSS v3.1: 9.8)
   【是否遭勒索軟體利用:未知□ Yii Framework存在對替代路徑保護不當的漏洞，可能允許遠端攻擊者執行任意程式碼。此漏洞可能影響其他採用Yii的產品，包括但不限於CVE-2025-32432所代表的Craft CMS□
   【影響平台】請參考官方所列的影響版本
   https://www.yiiframework.com/news/709/please-upgrade-to-yii-2-0-52

- 影響平台: 詳細內容於內容說明欄之影響平台
- 建議措施:
  1. □CVE-2025-1976□ 官方已針對漏洞釋出修復更新，請更新至相關版本
     https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25602
  2. □CVE-2025-42599□ 官方已針對漏洞釋出修復更新，請更新至相關版本
     https://www.qualitia.com/jp/news/2025/04/18_1030.html
  3. □CVE-2025-3928□ 官方已針對漏洞釋出修復更新，請更新至相關版本
     https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html
  4. □CVE-2025-31324□ 官方已針對漏洞釋出修復更新，請更新至相關版本
     https://me.sap.com/notes/3594142
  5. □CVE-2024-38475□ 官方已針對漏洞釋出修復更新，請更新至相關版本
     https://httpd.apache.org/security/vulnerabilities_24.html
  6. □CVE-2023-44221□ 官方已針對漏洞釋出修復更新，請更新至相關版本
     https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018
  7. □CVE-2025-34028□ 官方已針對漏洞釋出修復更新，請更新至相關版本
     https://documentation.commvault.com/securityadvisories/CV_2025_04_1.html
  8. □CVE-2024-58136□ 官方已針對漏洞釋出修復更新，請更新至相關版本
     https://www.yiiframework.com/news/709/please-upgrade-to-yii-2-0-52

計算機與通訊中心
網路系統組 敬啟