張貼日期：2025/05/22

【漏洞預警】CISA新增10個已知遭駭客利用之漏洞至KEV目錄(2025/05/12-2025/05/18)

- 主旨說明:【漏洞預警】CISA新增10個已知遭駭客利用之漏洞至KEV目錄(2025/05/12-2025/05/18)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202505-00000018

1. CVE-2025-47729【TeleMessage TM SGNL Hidden Functionality Vulnerability (CVSS v3.1: 4.9)
   - 【是否遭勒索軟體利用:未知】 TeleMessage TM SGNL存在隱藏功能漏洞，存檔後端將保留來自TM SGNL應用程式使用者的訊息明文副本。
   - 【影響平台】 TeleMessage archiving backend 2025-05-05(含)之前的版本
2. CVE-2025-32709【Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability (CVSS v3.1: 7.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows的WinSock輔助功能驅動程式存在記憶體釋放後使用漏洞，該漏洞允許經授權的攻擊者將權限提升至系統管理員。
   - 【影響平台】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32709
3. CVE-2025-30397【Microsoft Windows Scripting Engine Type Confusion Vulnerability (CVSS v3.1: 7.5)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows Scripting Engine存在類型混淆漏洞，該漏洞允許未經授權的攻擊者透過特製的URL在網路上執行程式碼。
   - 【影響平台】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30397
4. CVE-2025-32706【Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability (CVSS v3.1: 7.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows Common Log File System驅動程式存在堆積型緩衝區溢位漏洞，該漏洞允許經授權的攻擊者在本機提升權限。
   - 【影響平台】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32706
5. CVE-2025-32701【Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability (CVSS v3.1: 7.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows Common Log File System驅動程式存在記憶體釋放後使用漏洞，該漏洞允許經授權的攻擊者在本機提升權限。
   - 【影響平台】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32701
6. CVE-2025-30400【Microsoft Windows DWM Core Library Use-After-Free Vulnerability (CVSS v3.1: 7.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows DWM Core Library存在記憶體釋放後使用漏洞，該漏洞允許經授權的攻擊者在本機提升權限。
   - 【影響平台】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30400
7. CVE-2025-32756【Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 Fortinet的FortiFone、FortiVoice、FortiNDR和FortiMail存在堆疊緩衝區溢位漏洞，該漏洞可能允許未經驗證的遠端攻擊者透過特製的HTTP請求

執行任意程式碼或指令。
    - 【影響平台】請參考官方所列的影響版本 https://fortiguard.fortinet.com/psirt/FG-IR-25-254
8. CVE-2025-42999（SAP NetWeaver Deserialization Vulnerability (CVSS v3.1: 9.1)
    - 【是否遭勒索軟體利用:未知】 SAP NetWeaver Visual Composer Metadata Uploader存在反序列化漏洞，該漏洞允許具權限的攻擊者透過反序列化不信任或惡意的內容，危及主機系統的機密性、完整性和可用性。
    - 【影響平台】 SAP NetWeaver (Visual Composer development server) VCFRAMEWORK 7.50
9. CVE-2024-12987（DrayTek Vigor Routers OS Command Injection Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:未知】 DrayTek Vigor2960、Vigor300B和Vigor3900路由器存在作業系統指令注入漏洞，該漏洞源於Web管理介面apmcfgupload檔案的未知函式。
    - 【影響平台】請參考官方所列的影響版本
    - https://fw.draytek.com.tw/Vigor2960/Firmware/v1.5.1.5/DrayTek_Vigor2960_V1.5.1.5_01release-note.pdf
    - https://fw.draytek.com.tw/Vigor300B/Firmware/v1.5.1.5/DrayTek_Vigor300B_V1.5.1.5_01release-note.pdf
    - https://fw.draytek.com.tw/Vigor3900/Firmware/v1.5.1.5/DrayTek_Vigor3900_V1.5.1.5_01release-note.pdf
10. （CVE-2025-4664）Google Chromium Loader Insufficient Policy Enforcement Vulnerability (CVSS v3.1: 4.3)
    - 【是否遭勒索軟體利用:未知】 Google Chromium存在政策執行不足的漏洞，該漏洞允許遠端攻擊者透過特製的HTML頁面洩漏跨源資料。
    - 【影響平台】請參考官方所列的影響版本
    - https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html

- 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-2025-47729【 受影響的產品暫無有效緩解措施。建議使用者停止使用相關產品。
2. CVE-2025-32709【 官方已針對漏洞釋出修復更新，請更新至相關版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32709
3. CVE-2025-30397【 官方已針對漏洞釋出修復更新，請更新至相關版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30397
4. CVE-2025-32706【 官方已針對漏洞釋出修復更新，請更新至相關版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32706
5. CVE-2025-32701【 官方已針對漏洞釋出修復更新，請更新至相關版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32701
6. CVE-2025-30400【 官方已針對漏洞釋出修復更新，請更新至相關版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30400
7. CVE-2025-32756【 官方已針對漏洞釋出修復更新，請更新至相關版本 https://fortiguard.fortinet.com/psirt/FG-IR-25-254
8. CVE-2025-42999【 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/3604119
9. CVE-2024-12987【 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://fw.draytek.com.tw/Vigor2960/Firmware/v1.5.1.5/DrayTek_Vigor2960_V1.5.1.5_01release-note.pdf
    - https://fw.draytek.com.tw/Vigor300B/Firmware/v1.5.1.5/DrayTek_Vigor300B_V1.5.1.5_01release-note.pdf
    - https://fw.draytek.com.tw/Vigor3900/Firmware/v1.5.1.5/DrayTek_Vigor3900_V1.5.1.

5_01release-note.pdf

10. 【CVE-2025-4664】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html

---

計算機與通訊中心
網路系統組 敬啟