張貼日期：2025/11/05

【漏洞預警CISA新增8個已知遭駭客利用之漏洞至KEV目錄(2025/10/20-2025/10/26)

- 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(2025/10/20-2025/10/26)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202510-00000014

1. CVE-2022-48503Apple Multiple Products Unspecified Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知】 Apple macOSiOStvOSSafari 及 watchOS 中的 JavaScriptCore存在未具體說明的漏洞，當處理網頁內容時，可能導致任意程式碼執行。受影響的產品可能已達生命週期終止(EoL)或停止服務(EoS)建議使用者停止使用該產品。
   - 【影響平台】請參考官方所列的影響版本
   - https://support.apple.com/en-us/102879
   - https://support.apple.com/en-us/102893
   - https://support.apple.com/en-us/102878
   - https://support.apple.com/en-us/102891
   - https://support.apple.com/en-us/102892
2. CVE-2025-2746Kentico Xperience CMS Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 Kentico Xperience CMS 存在可透過替代路徑或通道繞過身份驗證漏洞Staging Sync Server 在摘要式驗證中對空白 SHA1 使用者名稱處理不當，攻擊者可能因此取得對管理物件的控制權。
   - 【影響平台】 Kentico Xperience 130.172之前的版本
3. CVE-2025-2747Kentico Xperience CMS Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 Kentico Xperience CMS 存在可透過替代路徑或通道繞過身份驗證漏洞，當 Staging Sync Server 組件在伺服器設定為None類型時存在密碼處理弱點，攻擊者可能因此取得對管理物件的控制權。
   - 【影響平台】 Kentico Xperience 130.178之前的版本
4. CVE-2025-33073Microsoft Windows SMB Client Improper Access Control Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows SMB 客戶端存在不當存取控制漏洞，攻擊者可誘導受害端主動建立到攻擊者的 SMB 連線並通過驗證，進而可能提升攻擊者在受害系統上的權限或執行未授權操作。
   - 【影響平台】請參考官方所列的影響版本
   - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073
5. CVE-2025-61884Oracle E-Business Suite Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 7.5)
   - 【是否遭勒索軟體利用:已知】 Oracle E-Business Suite 在 Oracle Configurator 的 Runtime 元件中存在伺服器端請求偽造漏洞。此漏洞可遠端被利用且無需驗證。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.oracle.com/security-alerts/alert-cve-2025-61884.html
6. CVE-2025-61932Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 Motex LANSCOPE Endpoint Manager存在通訊通道來源

驗證不當的漏洞，攻擊者可透過發送特製的封包來執行任意程式碼。
    - 【影響平台】請參考官方所列的影響版本
    - https://www.motex.co.jp/news/notice/2025/release251020/
7. CVE-2025-54236Adobe Commerce and Magento Improper Input Validation Vulnerability (CVSS v3.1: 9.1)
    - 【是否遭勒索軟體利用:未知】 Adobe Commerce 和 Magento Open Source 存在輸入驗證不當漏洞，攻擊者可能藉此透過 Commerce REST API 接管客戶帳戶。
    - 【影響平台】請參考官方所列的影響版本
    - https://helpx.adobe.com/security/products/magento/apsb25-88.html
8. CVE-2025-59287Microsoft Windows Server Update Service (WSUS) Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:未知】 Microsoft Windows Server Update ServiceWSUS存在反序列化不受信任資料漏洞，可能導致遠端程式碼執行。
    - 【影響平台】請參考官方所列的影響版本
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

- 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-2022-48503 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://support.apple.com/en-us/102879
    - https://support.apple.com/en-us/102893
    - https://support.apple.com/en-us/102878
    - https://support.apple.com/en-us/102891
    - https://support.apple.com/en-us/102892
2. CVE-2025-2746 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://devnet.kentico.com/download/hotfixes
3. CVE-2025-2747 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://devnet.kentico.com/download/hotfixes
4. CVE-2025-33073 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-2025-33073
5. CVE-2025-61884 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://www.oracle.com/security-alerts/alert-cve-2025-61884.html
6. CVE-2025-61932 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://www.motex.co.jp/news/notice/2025/release251020/
7. CVE-2025-54236 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://helpx.adobe.com/security/products/magento/apsb25-88.html
8. CVE-2025-59287 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-2025-59287

計算機與通訊中心
網路系統組 敬啟