張貼日期：2026/04/28

【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2026/04/06-2026/04/12)

- 主旨說明:【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2026/04/06-2026/04/12)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202604-00000013
  - 【CVE-2026-35616】Fortinet FortiClient EMS Improper Access Control Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Fortinet FortiClient EMS 存在不當存取控制漏洞，可能允許未經驗證的攻擊者透過特製的請求來執行未經授權的程式碼或指令。
  - 【CVE-2026-1340】Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager Mobile【EPMM】存在程式碼注入漏洞，可能允許攻擊者在未經驗證的情況下達成遠端程式碼執行。
  - 【CVE-2012-1854】Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Microsoft Visual Basic for Applications【VBA】存在不安全的函式庫載入漏洞，可能允許遠端程式碼執行。
  - 【CVE-2025-60710】Microsoft Windows Link Following Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Microsoft Windows 存在連結追蹤漏洞，可能導致權限提升。
  - 【CVE-2023-21529】Microsoft Exchange Server Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 Microsoft Exchange Server 存在不受信任資料反序列化漏洞，可能允許已通過驗證的攻擊者執行遠端程式碼。
  - 【CVE-2023-36424】Microsoft Windows Out-of-Bounds Read Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Microsoft Windows 通用日誌檔案系統驅動程式存在越界讀取漏洞，可能允許威脅行為者進行權限提升。
  - 【CVE-2020-9715】Adobe Acrobat Use-After-Free Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Adobe Acrobat 存在使用釋放後記憶體漏洞，可能允許程式碼執行。
  - 【CVE-2026-21643】Fortinet SQL Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Fortinet FortiClient EMS 存在 SQL 注入漏洞，可能允許未經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。
  - 【CVE-2026-34621】Adobe Acrobat and Reader Prototype Pollution Vulnerability (CVSS v3.1: 8.6)
  - 【是否遭勒索軟體利用:未知】 Adobe Acrobat and Reader 存在原型污染漏洞，可能允許任意程式碼執行。
- 影響平台:
  - 【CVE-2026-35616】請參考官方所列的影響版本 https://fortiguard.fortinet.com/psirt/FG-IR-26-099
  - 【CVE-2026-1340】請參考官方所列的影響版本 https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340
  - 【CVE-2012-1854】請參考官方所列的影響版本 https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-046

    - □CVE-2025-60710□請參考官方所列的影響版本
      https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710
    - □CVE-2023-21529□請參考官方所列的影響版本
      https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529
    - □CVE-2023-36424□請參考官方所列的影響版本
      https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36424
    - □CVE-2020-9715□請參考官方所列的影響版本
      https://helpx.adobe.com/security/products/acrobat/apsb20-48.html
    - □CVE-2026-21643□請參考官方所列的影響版本
      https://fortiguard.fortinet.com/psirt/FG-IR-25-1142
    - □CVE-2026-34621□請參考官方所列的影響版本
      https://helpx.adobe.com/security/products/acrobat/apsb26-43.html
- 建議措施:
    - □CVE-2026-35616□ 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-26-099
    - □CVE-2026-1340□ 官方已針對漏洞釋出修復更新，請更新至相關版本
      https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340
    - □CVE-2012-1854□ 官方已針對漏洞釋出修復更新，請更新至相關版本
      https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-046
    - □CVE-2025-60710□ 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-2025-60710
    - □CVE-2023-21529□ 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-2023-21529
    - □CVE-2023-36424□ 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-2023-36424
    - □CVE-2020-9715□ 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/acrobat/apsb20-48.html
    - □CVE-2026-21643□ 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-25-1142
    - □CVE-2026-34621□ 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/acrobat/apsb26-43.html

---

計算機與通訊中心
網路系統組 敬啟