張貼日期：2025/05/30

【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2025/05/19-2025/05/25)

- 主旨說明:【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2025/05/19-2025/05/25)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202505-00000022

1. 【CVE-2023-38950】ZKTeco BioTime Path Traversal Vulnerability (CVSS v3.1: 7.5)
   - 【是否遭勒索軟體利用:未知】 ZKTeco BioTime在其iclock API中存在路徑遍歷漏洞，該漏洞允許未經身份驗證的攻擊者透過提供特製的有效負載讀取任意檔案。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.zkteco.com/en/Security_Bulletinsibs/10
2. 【CVE-2024-27443】Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability (CVSS v3.1: 6.1)
   - 【是否遭勒索軟體利用:未知】 Zimbra Collaboration在Zimbra Webmail經典使用者介面的CalendarInvite功能中存在跨網站指令碼漏洞。攻擊者可透過包含特製的行事曆標頭的電子郵件訊息利用此漏洞，導致執行任意JavaScript程式碼。
   - 【影響平台】請參考官方所列的影響版本
   - https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes
   - https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P39#Security_Fixes
3. 【CVE-2025-27920】Srimax Output Messenger Directory Traversal Vulnerability (CVSS v3.1: 6.5)
   - 【是否遭勒索軟體利用:未知】 Srimax Output Messenger存在目錄遍歷漏洞，該漏洞允許攻擊者存取目標目錄以外的敏感檔案，可能導致組態洩漏或任意檔案存取。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.outputmessenger.com/cve-2025-27920/
4. 【CVE-2024-11182】MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability (CVSS v3.1: 6.1)
   - 【是否遭勒索軟體利用:未知】 MDaemon電子郵件伺服器存在跨網站指令碼漏洞，該漏洞允許遠端攻擊者透過HTML電子郵件載入任意JavaScript程式碼。
   - 【影響平台】請參考官方所列的影響版本
   - https://mdaemon.com/pages/downloads-critical-updates
5. 【CVE-2025-4428】Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager Mobile (EPMM) 的API元件中存在程式碼注入漏洞，該漏洞允許經身份驗證的攻擊者透過特製的API請求遠端執行任意程式碼。此漏洞源於對Hibernate Validator開源函式庫的不安全實作。
   - 【影響平台】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?language=en_US
6. 【CVE-2025-4427】Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability (CVSS v3.1: 7.5)
   - 【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager Mobile(EPMM)的API元件中存在身份驗證繞過漏洞，該漏洞允許攻擊者透過特製的API請求，在未提供適當憑證的情況下存取受保護的資源。此漏洞源於對Spring Framework開源函式庫的不安全實作。

        - 【影響平台】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?language=en_US
    7. CVE-2025-4632Samsung MagicINFO 9 Server Path Traversal Vulnerability (CVSS v3.1: 9.8)
        - 【是否遭勒索軟體利用:未知】 Samsung MagicINFO 9 Server存在路徑遍歷漏洞，該漏洞允許攻擊者以系統權限寫入任意檔案。
        - 【影響平台】請參考官方所列的影響版本
        - https://security.samsungtv.com/securityUpdates#SVP-MAY-2025
- 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-2023-38950 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://www.zkteco.com/en/Security_Bulletinsibs/10
    2. CVE-2024-27443 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes
        - https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P39#Security_Fixes
    3. CVE-2025-27920 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://www.outputmessenger.com/cve-2025-27920/
    4. CVE-2024-11182 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://mdaemon.com/pages/downloads-critical-updates
    5. CVE-2025-4428 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?language=en_US
    6. CVE-2025-4427 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?language=en_US
    7. CVE-2025-4632 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://security.samsungtv.com/securityUpdates#SVP-MAY-2025

計算機與通訊中心
網路系統組 敬啟