張貼日期：2025/04/08

【漏洞預警]CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2025/03/31-2025/04/06)

- 主旨說明:【漏洞預警]CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2025/03/31-2025/04/06)
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202504-00000002]
  -]CVE-2024-20439]Cisco Smart Licensing Utility Static Credential Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:未知] Cisco Smart Licensing Utility存在靜態憑證漏洞，該漏洞允許未經身份驗證的遠端攻擊者登入受影響的系統並取得管理憑證。
    - 【影響平台】請參考官方所列的影響版本https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw
  -]CVE-2025-24813]Apache Tomcat Path Equivalence Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:未知] Apache Tomcat存在路徑對等漏洞，該漏洞允許遠端攻擊者通過部分PUT請求執行程式碼、洩漏資訊或注入惡意內容。
    - 【影響平台】請參考官方所列的影響版本 https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq
  -]CVE-2025-22457]Ivanti Connect Secure, Policy Secure and ZTA Gateways Stack-Based Buffer Overflow Vulnerability (CVSS v3.1: 9.0)
    - 【是否遭勒索軟體利用:未知] Ivanti Connect Secure]Policy Secure和ZTA Gateways存在堆疊緩衝區溢位漏洞，該漏洞允許未經身份驗證的遠端攻擊者實現遠端程式碼執行。
    - 【影響平台】請參考官方所列的影響版本 https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US
  - 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-2024-20439] 官方已針對漏洞釋出修復更新，請更新至相關版本https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw
    2.]CVE-2025-24813] 官方已針對漏洞釋出修復更新，請更新至相關版本 https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq
    3.]CVE-2025-22457] 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/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US

計算機與通訊中心
網路系統組 敬啟