張貼日期：2025/04/21

【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/04/07-2025/04/13)

- 主旨說明:【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/04/07-2025/04/13)
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202504-00000007】
  - 【CVE-2025-31161】CrushFTP Authentication Bypass Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:已知】 CrushFTP在HTTP授權標頭中存在身份驗證繞過漏洞，允許遠端未經身份驗證的攻擊者以任何已知或可猜測的使用者帳戶(例如【crushadmin)進行身份驗證。
    - 【影響平台】請參考官方所列的影響版本 https://crushftp.com/crush11wiki/Wiki.jsp?page=Update#section-Update-VulnerabilityInfo
  - 【CVE-2025-29824】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:已知】 Microsoft Windows的通用日誌檔案系統(CLFS)驅動程式中存在記憶體釋放後使用漏洞，允許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-2025-29824
  - 【CVE-2025-30406】Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:未知】 Gladinet CentreStack存在使用硬體編碼加密金鑰漏洞，此漏洞與應用程式管理用於 ViewState完整性驗證的金鑰方式有關。若被成功利用，攻擊者可偽造用於伺服器端反序列化的ViewState有效負載，從而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://gladinetsupport.s3.us-east-1.amazonaws.com/gladinet/securityadvisory-cve-2005.pdf
  - 【CVE-2024-53150】Linux Kernel Out-of-Bounds Read Vulnerability (CVSS v3.1: 7.1)
    - 【是否遭勒索軟體利用:未知】 Linux Kernel在USB-audio驅動程式中存在越界讀取漏洞，該漏洞允許本機具備權限的攻擊者取得潛在的敏感資訊。
    - 【影響平台】
      - Linux 5.5 至5.10.231(不含)的版本
      - Linux 5.11 至5.15.174(不含)的版本
      - Linux 5.16 至6.1.120(不含)的版本
      - Linux 6.2 至6.6.64(不含)的版本
      - Linux 6.7 至6.11.11(不含)的版本
      - Linux 6.12 至6.12.2(不含)的版本
  - 【CVE-2024-53197】Linux Kernel Out-of-Bounds Access Vulnerability (CVSS v3.1: 7.8)
    - 【是否遭勒索軟體利用:未知】 Linux Kernel在USB-audio驅動程式中存在越界存取漏洞，該漏洞允許具有實體存取權限的攻擊者透過惡意USB裝置，竄改系統記憶體、提升權限或執行任意程式碼。
    - 【影響平台】
      - Linux 2.6.12 至4.19.325(不含)的版本
      - Linux 4.20 至5.4.287(不含)的版本
      - Linux 5.5 至5.10.231(不含)的版本
      - Linux 5.11 至5.15.174(不含)的版本
      - Linux 5.16 至6.1.120(不含)的版本

    - Linux 6.2 至6.6.64(不含)的版本
    - Linux 6.7 至6.11.11(不含)的版本
    - Linux 6.12 至6.12.2(不含)的版本
- 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-2025-31161 官方已針對漏洞釋出修復更新，請更新至相關版本
       https://crushftp.com/crush11wiki/Wiki.jsp?page=Update#section-Update-VulnerabilityInfo
    2. CVE-2025-29824 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-2025-29824
    3. CVE-2025-30406 官方已針對漏洞釋出修復更新，請更新至相關版本
       https://gladinetsupport.s3.us-east-1.amazonaws.com/gladinet/securityadvisory-cve-2005.pdf
    4. CVE-2024-53150 官方已針對漏洞釋出修復更新，請更新至相關版本
       https://git.kernel.org/stable/c/096bb5b43edf755bc4477e64004fa3a20539ec2f
       https://git.kernel.org/stable/c/45a92cbc88e4013bfed7fd2ccab3ade45f8e896b
       https://git.kernel.org/stable/c/74cb86e1006c5437b1d90084d22018da30fddc77
       https://git.kernel.org/stable/c/a3dd4d63eeb452cfb064a13862fb376ab108f6a6
       https://git.kernel.org/stable/c/a632bdcb359fd8145e86486ff8612da98e239acd
       https://git.kernel.org/stable/c/ab011f7439d9bbfd34fd3b9cef4b2d6d952c9bb9
       https://git.kernel.org/stable/c/da13ade87a12dd58829278bc816a61bea06a56a9
       https://git.kernel.org/stable/c/ea0fa76f61cf8e932d1d26e6193513230816e11d
    5. CVE-2024-53197 官方已針對漏洞釋出修復更新，請更新至相關版本
       https://git.kernel.org/stable/c/0b4ea4bfe16566b84645ded1403756a2dc4e0f19
       https://git.kernel.org/stable/c/379d3b9799d9da953391e973b934764f01e03960
       https://git.kernel.org/stable/c/62dc01c83fa71e10446ee4c31e0e3d5d1291e865
       https://git.kernel.org/stable/c/920a369a9f014f10ec282fd298d0666129379f1b
       https://git.kernel.org/stable/c/9887d859cd60727432a01564e8f91302d361b72b
       https://git.kernel.org/stable/c/9b8460a2a7ce478e0b625af7c56d444dc24190f7
       https://git.kernel.org/stable/c/b521b53ac6eb04e41c03f46f7fe452e4d8e9bcca
       https://git.kernel.org/stable/c/b8f8b81dabe52b413fe9e062e8a852c48dd0680d
       https://git.kernel.org/stable/c/b909df18ce2a998afef81d58bbd1a05dc0788c40

計算機與通訊中心
網路系統組 敬啟