張貼日期：2022/06/22

【資安漏洞預警】微軟支援診斷工具存在安全漏洞(CVE-2022-30190)□請儘速確認並進行更新

- 主旨說明：微軟支援診斷工具存在安全漏洞(CVE-2022-30190)□攻擊者可藉此遠端執行任意程式碼,請儘速確認並進行更新

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202206-0978□
  - 微軟支援診斷工具(Microsoft Support Diagnostic Tool, MSDT)為Windows作業系統用以蒐集裝置之診斷資料，並傳送給技術支援工程師以解決問題之工具。研究人員發現微軟支援診斷工具存在名為Follina之安全漏洞(CVE-2022-30190)□攻擊者誘騙使用者開啟惡意Word檔案時,可利用URL協定呼叫微軟支援診斷工具以觸發此漏洞，進而遠端執行任意程式碼。
- 影響平台：
  - Windows 7 for 32-bit Systems Service Pack 1
  - Windows 7 for x64-based Systems Service Pack 1
  - Windows 8.1 for 32-bit systems
  - Windows 8.1 for x64-based systems
  - Windows RT 8.1
  - Windows 10 for 32-bit Systems
  - Windows 10 for x64-based Systems
  - Windows 10 Version 1607 for 32-bit Systems
  - Windows 10 Version 1607 for x64-based Systems
  - Windows 10 Version 1809 for 32-bit Systems
  - Windows 10 Version 1809 for ARM64-based Systems
  - Windows 10 Version 1809 for x64-based Systems
  - Windows 10 Version 20H2 for 32-bit Systems
  - Windows 10 Version 20H2 for ARM64-based Systems
  - Windows 10 Version 20H2 for x64-based Systems
  - Windows 10 Version 21H1 for 32-bit Systems
  - Windows 10 Version 21H1 for ARM64-based Systems
  - Windows 10 Version 21H1 for x64-based Systems
  - Windows 10 Version 21H2 for 32-bit Systems
  - Windows 10 Version 21H2 for ARM64-based Systems
  - Windows 10 Version 21H2 for x64-based Systems
  - Windows 11 for ARM64-based Systems
  - Windows 11 for x64-based Systems
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1(Server Core installation)
  - Windows Server 2012
  - Windows Server 2012 (Server Core installation)
  - Windows Server 2012 R2
  - Windows Server 2012 R2(Server Core installation)
  - Windows Server 2016
  - Windows Server 2016(Server Core installation)
  - Windows Server 2019
  - Windows Server 2019(Server Core installation)

    - Windows Server 2022
    - Windows Server 2022(Server Core installation)
    - Windows Server, version 20H2(Server Core Installation)
- 建議措施：
    1. 目前微軟官方已針對此漏洞釋出更新程式，請各機關可聯絡系統維護廠商或參考以下連結進行更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190
    2. 若無法進行更新，可參考微軟官方網站採取下列緩解措施，以暫時關閉微軟支援診斷工具之URL協定：
        1. 以系統管理員身分開啟「命令提示字元」視窗
        2. 執行reg export HKEY_CLASSES_ROOTms-msdt filename指令進行機碼備份
        3. 執行指令reg delete HKEY_CLASSES_ROOTms-msdt /f
        4. 後續安裝修補程式後，若要還原機碼，請執行reg import filename
    3. 請更新電腦防毒軟體病毒碼。
    4. 請留意可疑電子郵件，注意郵件來源正確性，勿隨意點擊信件連結或開啟附件。
    5. 請加強內部宣導，提升人員資安意識，以防範駭客利用電子郵件進行社交工程攻擊。
- 參考資料：
    1. https://www.ithome.com.tw/news/151211
    2. https://www.ithome.com.tw/news/151238
    3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190
    4. https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
    5. https://support.microsoft.com/zh-tw/office/office-%E7%9A%84%E6%87%89%E7%94%A8%E7%A8%8B%E5%BC%8F%E9%98%B2%E8%AD%B7-9e0fb9c2-ffad-43bf-8ba3-78f785fdba46

計算機與通訊中心
網路系統組 敬啟