張貼日期：2022/01/21

【資安漏洞預警Microsoft 已發布安全更新，以解決多版本 Windows HTTP 遠端程式碼執行弱點，建議請管理者儘速評估更新！

- 主旨說明Microsoft 已發布安全更新，以解決多版本 Windows HTTP 遠端程式碼執行弱點，建議請管理者儘速評估更新！

- 內容說明：
  - 轉發 CHTSecurity 情資編號CHTSecurity-ANA-202201-0004
  - Microsoft 已發布安全更新，以解決多版本 Windows HTTP 遠端程式碼執行弱點。由於受影響系統的 (EnableTrailerSupport 註冊表值啟用 HTTP Trailer Support) 組件綁定到網路堆棧，未經身份驗證的攻擊者可利用 HTTP 協定堆棧 (http.sys) 將偽造封包發送到目標伺服器處理封包，進而可能造成遠端程式碼執行攻擊HiNet SOC 建議管理者儘速評估更新，以降低受駭風險。
- 影響平台:
  - Windows 10 Version 1809
  - Windows 10 Version 21H1
  - Windows 10 Version 20H2
  - Windows 10 Version 21H2
  - Windows 11 Windows Server 2019
  - Windows Server 2022
  - Windows Server version 20H2
- 建議措施:
  - 請參考說明或 Microsoft 官網將受影響版本的作修補更新(CVE-2022-21907)
    1. Windows 10 (1809、21H1、20H2、21H2)版本 (x86、x64、ARM64)
    2. Windows 11 (x64、ARM64)
    3. Windows Server (2019、2022)版本 (Base、Server Core)
    4. Windows Server (20H2)版本 (Server Core)
- 參考資料:
  1. https://github.com/antx-code/CVE-2022-21907
  2. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21907

計算機與通訊中心
網路系統組 敬啟