張貼日期：2021/05/14

【資安漏洞預警】微軟Hyper-V HTTP通訊協定堆疊及Object Linking and Embedding(OLE)存在安全漏洞

- 主旨：微軟Hyper-V HTTP通訊協定堆疊及Object Linking and Embedding(OLE)存在安全漏洞(CVE-2021-28476 CVE-2021-31166及CVE-2021-31194)允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

- 內容：
  1. 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202105-0389
  2. 微軟Hyper-V HTTP通訊協定堆疊及Object Linking and Embedding(OLE)存在安全漏洞(CVE-2021-28476 CVE-2021-31166及CVE-2021-31194)可能遭遠端攻擊者藉由發送特製封包或誘騙受害者存取特製網頁，進而利用漏洞執行任意程式碼。

- 影響平台：
  受影響版本如下：
  - CVE-2021-28476
    - Windows 7 for x64-based Systems Service Pack 1;
    - Windows 8.1 for x64-based systems;
    - Windows 10 for x64-based Systems;
    - Windows 10 Version 1607 for x64-based Systems;
    - Windows 10 Version 1803 for x64-based Systems;
    - Windows 10 Version 1809 for x64-based Systems;
    - Windows 10 Version 1909 for x64-based Systems;
    - Windows 10 Version 2004 for x64-based Systems;
    - Windows 10 Version 20H2 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 2008 for x64-based Systems Service Pack 2;
    - Windows Server 2008 for x64-based Systems Service Pack 2 (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, version 1909 (Server Core installation);
    - Windows Server, version 2004 (Server Core installation);
    - Windows Server, version 20H2 (Server Core Installation);
  - CVE-2021-31166;
    - Windows 10 Version 2004 for ARM64-based Systems;

        - Windows 10 Version 2004 for 32-bit Systems;
        - Windows 10 Version 2004 for x64-based Systems;
        - Windows 10 Version 20H2 for ARM64-based Systems;
        - Windows 10 Version 20H2 for 32-bit Systems;
        - Windows 10 Version 20H2 for x64-based Systems;
        - Windows Server, version 2004 (Server Core installation);
        - Windows Server, version 20H2 (Server Core Installation);
    - CVE-2021-31194□;
        - 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 1803 for ARM64-based Systems;
        - Windows 10 Version 1803 for 32-bit Systems;
        - Windows 10 Version 1803 for x64-based Systems;
        - Windows 10 Version 1809 for ARM64-based Systems;
        - Windows 10 Version 1809 for 32-bit Systems;
        - Windows 10 Version 1809 for x64-based Systems;
        - Windows 10 Version 1909 for ARM64-based Systems;
        - Windows 10 Version 1909 for 32-bit Systems;
        - Windows 10 Version 1909 for x64-based Systems;
        - Windows 10 Version 2004 for ARM64-based Systems;
        - Windows 10 Version 2004 for 32-bit Systems;
        - Windows 10 Version 2004 for x64-based Systems;
        - Windows 10 Version 20H2 for ARM64-based Systems;
        - Windows 10 Version 20H2 for 32-bit Systems;
        - Windows 10 Version 20H2 for x64-based Systems;
        - Windows Server 2008 for 32-bit Systems Service Pack 2;
        - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation);
        - Windows Server 2008 for x64-based Systems Service Pack 2;
        - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation);
        - 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, version 1909 (Server Core installation);
        - Windows Server, version 2004 (Server Core installation);
        - Windows Server, version 20H2 (Server Core Installation);

- 建議措施：
  目前微軟官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商或參考以下網址進行更新：
  1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28476
  2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31166
  3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31194
- 參考資料：
  1. https://www.ithome.com.tw/news/144350
  2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28476
  3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31166
  4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31194

計算機與通訊中心
網路系統組 敬啟