張貼日期：2023/05/16

【資安漏洞預警】微軟釋出5月份安全性更新，修補3個零時差漏洞(CVE-2023-29325、CVE-2023-29336及CVE-2023-24932)與2個高風險漏洞(CVE-2023-24941與CVE-2023-24943)、請儘速確認並進行更新或評估採取緩解措施

- 主旨說明：微軟釋出5月份安全性更新，修補3個零時差漏洞(CVE-2023-29325、CVE-2023-29336及CVE-2023-24932)與2個高風險漏洞(CVE-2023-24941與CVE-2023-24943)、其中2個漏洞已遭駭客利用，請儘速確認並進行更新或評估採取緩解措施

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202305-0234、
  - 微軟於5月份安全性更新中，共修補3個零時差漏洞與2個CVSS為9.8分高風險漏洞，請儘速確認並進行更新或評估採取緩解措施。
    1. CVE-2023-29325(CVSS 8.1)為遠端執行任意程式碼漏洞，攻擊者可寄送刻意變造之電子郵件，當受駭者使用Outlook開啟或預覽惡意RTF文件時，便會觸發漏洞進而達到遠端執行任意程式碼。
    2. CVE-2023-29336(CVSS7.8)為權限擴張漏洞，已遭駭客利用，發生於Win32K驅動程式，允許已通過身分鑑別之攻擊者，可透過本漏洞取得系統權限。
    3. CVE-2023-24932(CVSS 6.7)為安全功能繞過漏洞，已遭駭客利用，允許已取得本機管理權限之攻擊者，可透過本漏洞繞過安全開機(Windows Secure Boot)檢查機制，規避偵測或企圖使惡意程式進駐於系統中。
    4. CVE-2023-24941(CVSS 9.8)為遠端執行任意程式碼漏洞，允許未經身分鑑別之遠端攻擊者，針對網路檔案系統(Network File System, NFS)發送偽造請求，進而達到遠端執行任意程式碼。
    5. CVE-2023-24943(CVSS 9.8)為遠端執行任意程式碼漏洞，可使攻擊者藉由發送惡意檔案至啟用訊息佇列服務(Message Queuing Service)之實際通用多播(Pragmatic General Multicast)伺服器環境，進而達到遠端執行任意程式碼。
- 影響平台：
  - 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 21H2 for 32-bit Systems
  - Windows 10 Version 21H2 for ARM64-based Systems

    - Windows 10 Version 21H2 for x64-based Systems
    - Windows 10 Version 22H2 for 32-bit Systems
    - Windows 10 Version 22H2 for ARM64-based Systems
    - Windows 10 Version 22H2 for x64-based Systems
    - Windows 11 version 21H2 for ARM64-based Systems
    - Windows 11 version 21H2 for x64-based Systems
    - Windows 11 Version 22H2 for ARM64-based Systems
    - Windows 11 Version 22H2 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 2022
    - Windows Server 2022 (Server Core installation)
- 建議措施：
    - 目前微軟官方已針對弱點釋出修復版本，各機關可聯絡系統維護廠商進行修補，或參考以下連結進行緩解與取得修補程式：
        1. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29325
        2. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29336
        3. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24932
        4. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24941
        5. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24943
- 參考資料：
    1. https://www.zerodayinitiative.com/blog/2023/5/8/the-may-2023-security-update-review
    2. https://www.ithome.com.tw/news/156822
    3. https://msrc.microsoft.com/update-guide/releaseNote/2023-May
    4. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29325
    5. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29336
    6. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24932
    7. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24941
    8. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24943

—- 計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20230516_01

Last update: **2023/05/16 15:22**