張貼日期：2023/04/17

【漏洞預警】微軟通用紀錄檔系統(CLFS)驅動程式存在權限提升之高風險安全漏洞(CVE-2023-28252)，請儘速確認並進行更新或評估採取緩解措施

- 主旨說明：微軟通用紀錄檔系統(CLFS)驅動程式存在權限提升之高風險安全漏洞(CVE-2023-28252)，允許已取得一般權限之攻擊者提升至系統權限，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-202304-0734，
  - 研究人員發現微軟通用紀錄檔系統(Common Log File System, CLFS)驅動程式存在權限提升(Elevation of Privilege)之高風險安全漏洞(CVE-2023-28252)，允許已取得系統一般權限且可於系統執行程式之攻擊者進一步取得系統(System)權限。本漏洞已於本年2月遭駭客利用並部署勒索軟體Nokoyawa，美國網路安全暨基礎設施安全局(CISA)亦將此漏洞列為優先修補對象。
- 影響平台:
  - 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 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安全性更新(包含於4月份之彙總更新中)，各機關可自行或聯絡系統維護廠商進行修補，修補程式連結如下：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252

- 參考資料:
    1. https://www.ithome.com.tw/news/156373
    2. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252
    3. https://nvd.nist.gov/vuln/detail/CVE-2023-28252

計算機與通訊中心
網路系統組 敬啟