

張貼日期：2024/05/09

【漏洞預警】Microsoft SmartScreen Prompt存在高風險安全漏洞(CVE-2024-29988)請儘速確認並進行修補！

- 主旨說明Microsoft SmartScreen Prompt存在高風險安全漏洞(CVE-2024-29988)請儘速確認並進行修補！
- 內容說明:
 - 轉發 國家資安資訊分享與分析中心 NISAC-200-202405-00000032
 - 研究人員發現Microsoft SmartScreen Prompt存在保護機制失效(Protection Mechanism Failure)漏洞(CVE-2024-29988)攻擊者可利用此漏洞製作惡意網路捷徑檔案，受駭者下載並點擊該檔案後，將繞過SmartScreen告警執行來源不明檔案之機制，使惡意程式可於受駭者未察覺之情況下背景執行。該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
 - 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 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 11 Version 23H2 for ARM64-based Systems
 - Windows 11 Version 23H2 for x64-based Systems
 - Windows Server 2019
 - Windows Server 2019 (Server Core installation)
 - Windows Server 2022
 - Windows Server 2022 (Server Core installation)
 - Windows Server 2022, 23H2 Edition (Server Core installation)
- 建議措施:
 - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988>
- 參考資料:
 1. <https://nvd.nist.gov/vuln/detail/CVE-2024-20353>
 2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988>

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/announcement:20240509_03



Last update: **2024/05/09 16:11**