張貼日期：2023/04/07

【資安漏洞預警】微軟Outlook存在權限擴張之高風險安全漏洞(CVE-2023-23397)允許遠端攻擊者取得受駭者身分鑑別雜湊值，進而執行偽冒身分攻擊，請儘速確認並進行更新或評估採取緩解措施！

主旨：微軟Outlook存在權限擴張之高風險安全漏洞(CVE-2023-23397)允許遠端攻擊者取得受駭者身分鑑別雜湊值，進而執行偽冒身分攻擊，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-202304-0215
  - 研究人員發現微軟Outlook存在權限擴張(Elevation of Privilege)之高風險安全漏洞(CVE-2023-23397)遠端攻擊者可透過寄送附帶提醒的惡意郵件，當受駭者開啟Outlook並跳出提醒通知後，系統將於無任何互動指令之情況下，自動將Net-NTLMv2身分鑑別雜湊資訊傳送予攻擊者，攻擊者即可利用偽冒受駭者身分存取服務或破解雜湊值取得受駭者通行碼。
- 影響平台：
  - Microsoft 365 Apps for Enterprise for 32-bit Systems
  - Microsoft 365 Apps for Enterprise for 64-bit Systems
  - Microsoft Office 2019 for 32-bit editions
  - Microsoft Office 2019 for 64-bit editions
  - Microsoft Office LTSC 2021 for 32-bit editions
  - Microsoft Office LTSC 2021 for 64-bit editions
  - Microsoft Outlook 2013 RT Service Pack 1
  - Microsoft Outlook 2013 Service Pack 1(32-bit editions)
  - Microsoft Outlook 2013 Service Pack 1(64-bit editions)
  - Microsoft Outlook 2016(32-bit edition)
  - Microsoft Outlook 2016(64-bit edition)
- 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，或參考以下連結取得修補程式：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23397

- 參考資料：
  1. https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/
  2. https://www.ithome.com.tw/news/155952
  3. https://www.xmcyber.com/blog/cve-2023-23397-outlook-vulnerability/
  4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
  5. https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10386

—- 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:20230407_03

Last update: **2023/04/10 14:35**