

張貼日期：2023/09/14

【漏洞預警】WinRAR存在安全漏洞(CVE-2023-38831)請儘速確認並進行更新或評估採取緩解措施

- 主旨說明WinRAR存在安全漏洞(CVE-2023-38831)允許攻擊者遠端執行任意程式碼，該漏洞目前已遭駭客利用，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-200-202309-00000016
 - 研究人員發現WinRAR存在安全漏洞(CVE-2023-38831)由於ZIP文件處理過程不當，攻擊者可製作惡意ZIP或RAR壓縮檔，內容包含正常檔案與存有惡意執行檔之同名資料夾，當受駭者遭誘騙開啟正常檔案時，同名資料夾內之惡意執行檔將會觸發執行，進而遠端執行任意程式碼，相關研究表示該漏洞在本年4月已遭駭客利用。
- 影響平台：
 - WinRAR 6.22以下版本
- 建議措施：
 - 更新WinRAR至6.23以上版本，步驟如下：
 1. 開啟WinRAR
 2. 說明(關於WinRAR首頁)
 3. 進入首頁下載WinRAR 6.23以上版本進行替代
- 參考資料：
 1. <https://nvd.nist.gov/vuln/detail/CVE-2023-38831>
 2. <https://www.win-rar.com/>
 3. <https://www.ithome.com.tw/news/158421>

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/mailling:announcement:20230914_01

Last update: 2023/09/14 16:49

