

張貼日期：2024/06/19

【漏洞預警】Justice AV Solutions Viewer存在高風險安全漏洞(CVE-2024-4978)請儘速確認並進行修補

- 主旨說明 Justice AV Solutions Viewer存在高風險安全漏洞(CVE-2024-4978)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-200-202406-00000128
 - 研究人員發現Justice AV Solutions Viewer 8.3.7.250-1安裝程式被植入後門程式(CVE-2024-4978)受駭者從官網下載並安裝Justice AV Solutions Viewer後，後門程式會一併安裝並於背景執行未經授權之PowerShell指令。該漏洞已遭駭客利用，請儘速確認並進行更新。
- 影響平台：
 - JAVS Viewer v8.3.7.250-1
- 建議措施：
 - 官方已針對漏洞釋出更新，請更新至以下版本 JAVS Viewer v8.3.8(含)以後版本
- 參考資料：
 1. <https://nvd.nist.gov/vuln/detail/CVE-2024-4978/>
 2. <https://www.javs.com/downloads/>
 3. <https://www.rapid7.com/blog/post/2024/05/23/cve-2024-4978-backdoored-justice-av-solutions-viewer-software-used-in-apparent-supply-chain-attack/>

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:20240619_01



Last update: 2024/06/19 14:40