

張貼日期：2026/03/11

【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2026/03/02-2026/03/08)

- 主旨說明: 【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2026/03/02-2026/03/08)
- 內容說明:
 - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202603-00000007
 - [CVE-2026-22719]Broadcom VMware Aria Operations Command Injection Vulnerability (CVSS v3.1: 8.1)
 - 【是否遭勒索軟體利用:未知】Broadcom VMware Aria Operations 存在指令注入漏洞，未經驗證的攻擊者可利用此漏洞執行任意指令，可能在支援輔助產品遷移時導致遠端程式碼執行。
 - [CVE-2026-21385]Qualcomm Multiple Chipsets Memory Corruption Vulnerability (CVSS v3.1: 7.8)
 - 【是否遭勒索軟體利用:未知】多款 Qualcomm 晶片組在進行記憶體配置對齊時存在記憶體毀損漏洞。
 - [CVE-2017-7921]Hikvision Multiple Products Improper Authentication Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】多款 Hikvision 產品存在不當身分驗證漏洞，惡意使用者可能藉此提升系統權限並存取敏感資訊。
 - [CVE-2021-22681]Rockwell Multiple Products Insufficient Protected Credentials Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】多款 Rockwell 產品存在憑證保護不足漏洞[Studio 5000 Logix Designer 軟體中的一組金鑰可能被發現，而該金鑰用於驗證 Logix 控制器與 Rockwell Automation 設計軟體之間的通訊。若成功利用此漏洞，未經授權的應用程式可能連線至 Logix 控制器。
 - [CVE-2023-43000]Apple Multiple products Use-After-Free Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】Apple macOS[iOS]iPadOS 與 Safari 16.6 存在記憶體釋放後使用漏洞。當系統處理惡意構造的網頁內容時，可能導致記憶體毀損。
 - [CVE-2021-30952]Apple Multiple Products Integer Overflow or Wraparound Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】Apple tvOS[macOS]Safari[iPadOS 與 watchOS 存在整數溢位或回繞漏洞。當系統處理惡意構造的網頁內容時，可能導致任意程式碼執行。
 - [CVE-2023-41974]Apple iOS and iPadOS Use-After-Free Vulnerability (CVSS v3.1: 7.8)
 - 【是否遭勒索軟體利用:未知】Apple iOS 與 iPadOS 存在記憶體釋放後使用漏洞，應用程式可能藉此以核心權限執行任意程式碼。
- 影響平台:
 - [CVE-2026-22719]請參考官方所列的影響版本
 - <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947>
 - [CVE-2026-21385]請參考官方所列的影響版本
 - <https://docs.qualcomm.com/securitybulletin/march-2026-bulletin.html>
 - [CVE-2017-7921]請參考官方所列的影響版本
 - <https://www.hikvision.com/us-en/support/document-center/special-notices/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/>
 - [CVE-2021-22681]請參考官方所列的影響版本
 - <https://www.cisa.gov/news-events/ics-advisories/icsa-21-056-03>

- [CVE-2023-43000]請參考官方所列的影響版本
- <https://support.apple.com/en-us/120324>
- <https://support.apple.com/en-us/120331>
- <https://support.apple.com/en-us/120338>
- [CVE-2021-30952]請參考官方所列的影響版本
- <https://support.apple.com/en-us/HT212975>
- <https://support.apple.com/en-us/HT212976>
- <https://support.apple.com/en-us/HT212978>
- <https://support.apple.com/en-us/HT212980>
- <https://support.apple.com/en-us/HT212982>
- [CVE-2023-41974]請參考官方所列的影響版本
- <https://support.apple.com/en-us/HT213938>
- 建議措施:
 - [CVE-2026-22719] 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947>
 - [CVE-2026-21385] 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://docs.qualcomm.com/securitybulletin/march-2026-bulletin.html>
 - [CVE-2017-7921] 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://www.hikvision.com/us-en/support/document-center/special-notice/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/>
 - [CVE-2021-22681] 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://www.cisa.gov/news-events/ics-advisories/icsa-21-056-03>
 - [CVE-2023-43000] 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://support.apple.com/en-us/120324>
 - <https://support.apple.com/en-us/120331>
 - <https://support.apple.com/en-us/120338>
 - [CVE-2021-30952] 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://support.apple.com/en-us/HT212975>
 - <https://support.apple.com/en-us/HT212976>
 - <https://support.apple.com/en-us/HT212978>
 - <https://support.apple.com/en-us/HT212980>
 - <https://support.apple.com/en-us/HT212982>
 - [CVE-2023-41974] 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://support.apple.com/en-us/HT213938>

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:20260311_21



Last update: **2026/03/11 14:26**