張貼日期：2026/03/11

【漏洞預警】Broadcom VMware存在高風險安全漏洞(CVE-2026-22719與CVE-2026-22720)，請儘速確認並進行修補

- 主旨說明:【漏洞預警】Broadcom VMware存在高風險安全漏洞(CVE-2026-22719與CVE-2026-22720)，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 資安訊息警訊 NISAC-200-202603-00000006
  - 研究人員發現Broadcom VMware存在2項高風險安全漏洞(CVE-2026-22719與CVE-2026-22720)，類型分別為指令注入(Command Injection)與儲存型跨網站腳本攻擊(Stored Cross-Site Scripting)，前者於Aria Operations支援協助產品遷移(support-assisted product migration)流程中，可使未經身分鑑別之遠端攻擊者利用此漏洞於受影響設備執行任意指令，此漏洞已遭駭客利用；後者可使具建立自訂評估標準(custom benchmark)權限之遠端攻擊者注入惡意腳本，進而以管理者權限執行系統操作。請儘速確認並進行修補。
- 影響平台:
  - VMware Aria Operations 8.05至8.18.6(不含)以前版本
  - VMware Cloud Foundation 4.0至5.2.3(不含)以前版本
  - VMware Cloud Foundation 9.0至9.0.2.0(不含)以前版本
  - VMware Telco Cloud Platform 4.0至5.1(含)以前版本
  - VMware Telco Cloud Infrastructure 2.2至3.0(含)以前版本
- 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://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-22719
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-22720
  3. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947

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:20260311_23

Last update: **2026/03/11 14:50**