張貼日期：2026/08/03

【漏洞預警VMware多項產品存在3項高風險安全漏洞(CVE-2026-47876、CVE-2026-59309及CVE-2026-59310)，請儘速確認並進行修補

- 主旨說明:【漏洞預警VMware多項產品存在3項高風險安全漏洞(CVE-2026-47876、CVE-2026-59309及CVE-2026-59310)，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-200-202608-00000001
  - 研究人員發現VMware多項產品存在3項高風險安全漏洞(CVE-2026-47876、CVE-2026-59309及CVE-2026-59310)，類型分別為越界寫入(Out-of-Bounds Write)、身分鑑別繞過(Authentication Bypass)及路徑遍歷(Path Traversal)，請儘速確認並進行修補。
  - CVE-2026-47876，已取得虛擬機器VMXNET3介面卡本機管理員權限之攻擊者，可於ESXi主機上執行任意程式碼， CVE-2026-59309，已取得VMware vCenter網路存取權限之遠端攻擊者，可利用此漏洞於未經授權之情況下繞過身分鑑別並存取系統。
  - CVE-2026-59310，已取得VMware vCenter網路存取權限之遠端攻擊者，可利用此漏洞執行任意程式碼。
- 影響平台:
  - VMware Cloud Foundation 5.x版本至8.0 U3k(不含)版本
  - VMware Cloud Foundation與VMware vSphere Foundation 9.0.x.x版本
  - VMware Cloud Foundation與VMware vSphere Foundation 9.1.x.x版本
  - VMware vCenter 8.0
  - VMware Telco Cloud Platform 3.0版本
  - VMware Telco Cloud Platform 4.x版本
  - VMware Telco Cloud Platform 5.0.x版本
  - VMware Telco Cloud Platform 5.1.x版本
  - VMware Telco Cloud Infrastructure 3.0版本
  - VMware ESX 8.0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/0/38017
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-47876
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-59309
  3. https://nvd.nist.gov/vuln/detail/CVE-2026-59310
  4. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

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:20260803_22

Last update: **2026/08/03 14:18**