張貼日期：2026/08/20

【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2026/08/10-2026/08/16)

- 主旨說明:【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2026/08/10-2026/08/16)

- 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-200-202608-00000013
  - 【CVE-2026-20349】Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Heap Inspection Vulnerability (CVSS v3.1: 8.6)
  - 【是否遭勒索軟體利用:未知】 Cisco Secure Firewall Adaptive Security Appliance(ASA)及Secure Firewall Threat Defense(FTD)存在堆積檢查漏洞，未經驗證的遠端攻擊者可利用此漏洞導致設備意外重新載入，進而引發阻斷服務狀況。
  - 【CVE-2026-68820】Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability (CVSS v3.1: 7.0)
  - 【是否遭勒索軟體利用:未知】 Microsoft Windows WinSock輔助功能驅動程式存在使用釋放後記憶體漏洞，經授權的攻擊者可利用此漏洞在本機提升權限。
  - 【CVE-2026-72898】Metabase SQL Injection Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 Metabase存在SQL注入漏洞，未經驗證的遠端攻擊者可利用此漏洞，將任意SQL指令注入 Metabase應用程式資料庫，進而取得該執行個體的管理員權限。攻擊者取得權限後，可能進一步修改應用程式設定、竊取連線資料庫已儲存的憑證、讀取透過這些連線所能存取的任何資料並匯出。
- 影響平台:
  - 【CVE-2026-20349】請參考官方所列的影響版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF
  - 【CVE-2026-68820】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820
  - 【CVE-2026-72898】請參考官方所列的影響版本 https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf
- 建議措施:
  - 【CVE-2026-20349】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF
  - 【CVE-2026-68820】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820
  - 【CVE-2026-72898】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf

---

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:20260820_21

Last update: **2026/08/20 11:22**