張貼日期：2026/04/02

【漏洞預警□CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2026/03/23-2026/03/29)

- 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(2026/03/23-2026/03/29)

- 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-200-202603-00000023
  - □CVE-2026-33017□Langflow Code Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知□ Langflow 存在程式碼注入漏洞，可能導致在無需驗證的情況下建立公開流程。
  - □CVE-2026-33634□Aquasecurity Trivy Embedded Malicious Code Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知□ Aquasecurity Trivy 存在嵌入式惡意程式碼漏洞，可能使攻擊者取得 CI/CD 環境中的所有存取權限，包括所有權杖□SSH 金鑰、雲端憑證、資料庫密碼，以及記憶體中的任何敏感設定。
  - □CVE-2025-53521□F5 BIG-IP Unspecified Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知□ F5 BIG-IP AMP 存在未具體說明的漏洞，可能使攻擊者得以執行遠端程式碼。
- 影響平台:
  - □CVE-2026-33017□請參考官方所列的影響版本 https://github.com/langflow-ai/langflow/security/advisories/GHSA-vwmf-pq79-vjvx
  - □CVE-2026-33634□請參考官方所列的影響版本 https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23
  - □CVE-2025-53521□請參考官方所列的影響版本 https://my.f5.com/manage/s/article/K000156741
- 建議措施:
  - □CVE-2026-33017□ 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/langflow-ai/langflow/security/advisories/GHSA-vwmf-pq79-vjvx
  - □CVE-2026-33634□ 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23
  - □CVE-2025-53521□ 官方已針對漏洞釋出修復更新，請更新至相關版本 https://my.f5.com/manage/s/article/K000156741

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:20260402_23

Last update: **2026/04/02 09:44**