張貼日期：2025/03/26

【漏洞預警】Kubernetes 的 ingress-nginx 存在多個重大資安漏洞

- 主旨說明:【漏洞預警】Kubernetes 的 ingress-nginx 存在多個重大資安漏洞
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202503-00000012】
  - Kubernetes (K8s)是由Google設計用來自動化部屬、擴展與管理容器化的系統，可以集群的方式運行和管理容器，實現高效率的建置。近日揭露Kubernetes的ingress-nginx存在四個重大資安漏洞。
  - 【CVE-2025-24514】CVSS：8.8】 此漏洞為auth-url的註解可注入至nginx】可能導致在ingress-nginx控制器的上下文中執行任意程式碼，並洩漏控制器存取的資料。
  - 【CVE-2025-1097】CVSS：8.8】 此漏洞為auth-tls-match-cn的註解可注入至nginx】可能導致在ingress-nginx控制器的上下文中執行任意程式碼，並洩漏控制器存取的資料。
  - 【CVE-2025-1098】CVSS：8.8】 此漏洞為mirror-target和mirror-host的註解可注入至nginx】可能導致在ingress-nginx控制器的上下文中執行任意程式碼，並洩漏控制器存取的資料。
  - 【CVE-2025-1974】CVSS：9.8】 此漏洞允許未經過身分驗證的攻擊者可存取Pod網路，在ingress-nginx控制器的上下文中執行任意程式碼，可能導致洩漏控制器的資料。
- 影響平台:
  - Kubernetes ingress-nginx 1.11.0 之前版本
  - Kubernetes ingress-nginx 1.11.0 - 1.11.4
  - Kubernetes ingress-nginx 1.12.0
- 建議措施: 更新至以下版本：
  - Kubernetes ingress-nginx 1.11.5】
  - Kubernetes ingress-nginx 1.12.1
- 參考資料: https://www.twcert.org.tw/tw/cp-169-10026-1ab72-1.html

---

計算機與通訊中心
網路系統組 敬啟