

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2025032609031515	發佈時間	2025-03-26 09:29:16
事故類型	ANA-漏洞預警	發現時間	2025-03-26 09:20:16
影響等級	中		

[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。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

[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>