Boletín de alerta

Boletín Nro.:
Fecha de publicación: 25/03/2025
Tema: Alerta 2025-26 Ataque sin autenticación en Kubernetes
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

k8s.io/ingress-nginx (Go)
• < 1.11.5 • >= 1.12.0-beta.0, < 1.12.1

Descripción

Se ha descubierto un conjunto de cinco vulnerabilidades críticas en Ingress NGINX para Kubernetes, identificadas colectivamente como «IngressNightmare». Estas fallas permiten la ejecución remota de código no autenticado, comprometiendo más de 6,500 clústeres expuestos a Internet. Las vulnerabilidades, registradas bajo los identificadores CVE-2025-24513, CVE-2025-24514, CVE-2025-1097, CVE-2025-1098 y CVE-2025-1974, tienen una puntuación CVSS de hasta 9.8, lo que las clasifica como críticas. No afectan a NGINX Ingress Controller para NGINX y NGINX Plus.

El ataque se basa en explotar la falta de autenticación en los controladores de admisión dentro de los pods de Kubernetes. Un atacante puede inyectar configuraciones maliciosas en NGINX a través de objetos de ingreso manipulados, lo que permite la ejecución de código en el pod del controlador.

Dado que el controlador de admisión opera con privilegios elevados y acceso irrestricto a la red, un atacante exitoso podría ejecutar comandos arbitrarios, acceder a secretos del clúster y, potencialmente, tomar el control total del entorno Kubernetes.

Lista de vulnerabilidades y riesgos:
• CVE-2025-24513 (CVSS 4.8): Entrada no validada que puede provocar un recorrido de directorio, lo que facilita ataques de Denegación de Servicio (DoS) o filtración parcial de secretos.
• CVE-2025-24514 (CVSS 8.8): Uso indebido de la anotación auth-url para inyectar configuraciones maliciosas en NGINX, permitiendo ejecución de código y robo de secretos.
• CVE-2025-1097 (CVSS 8.8): Explotación de auth-tls-match-cn para modificar la configuración de NGINX, lo que habilita la ejecución de código arbitrario.
• CVE-2025-1098 (CVSS 8.8): Uso de mirror-target y mirror-host para alterar la configuración de NGINX y comprometer el controlador.

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 25/03/2025
Tema: Alerta 2025-26 Ataque sin autenticación en Kubernetes
Traffic Light Protocol (TLP): Amber

• CVE-2025-1974 (CVSS 9.8): Ataque sin autenticación que permite ejecución remota de código si el atacante tiene acceso a la red de pods.

Solución

• Actualizar a Ingress NGINX 1.11.5 o 1.12.1 para corregir las vulnerabilidades.

Información adicional:
• https://www.wiz.io/blog/ingress-nginx-kubernetes-vulnerabilities
• https://thehackernews.com/2025/03/critical-ingress-nginx-controller.html