Image Security

Docker Image Security

Una imagen vulnerable puede albergar amenazas de seguridad, permitiendo la explotación de vulnerabilidades.

Buenas prácticas:

1. Utilizar imágenes base mínimas y de confianza.
2. Reconstruir regularmente las imágenes.
3. Utilizar escáneres de imágenes.
4. Utilizar Docker content trust para verificar la autenticidad de la imagen.
5. Lint Dockerfiles para detectar errores de configuración inseguros.

1. Utilizar imágenes mínimas y de confianza

- Puedes encontrar estas imágenes filtrando mediante las opciones «Docker Official Image» y «Verified Publisher» en Docker Hub.

- También es aconsejable utilizar imágenes mínimas (como las variantes basadas en Alpine) siempre que sea posible. Estas deberían contener menos paquetes, lo que reduce su superficie de ataque.

2. Reconstruir regularmente las imágenes.

- Reconstruye regularmente tus imágenes para asegurarte de que incluyen paquetes y dependencias actualizados.

- Las imágenes construidas son inmutables, por lo que las correcciones de errores de paquetes y los parches de seguridad publicados después de su construcción no llegarán a sus contenedores en ejecución.

- Puedes automatizar el proceso de sustitución de contenedores utilizando una herramienta como Watchtower.

3. Utilizar escáneres de vulnerabilidad de imágenes

- Las herramientas de exploración son capaces de identificar qué paquetes está utilizando, si contienen alguna vulnerabilidad y cómo puede solucionar el problema actualizando o eliminando el paquete.

- Es una buena idea incluir estos escaneos como trabajos en tu CI pipeline.

4. Docker content trust

- Antes de iniciar un contenedor, debe asegurarse de que la imagen que está utilizando es auténtica. Un atacante podría haber subido un reemplazo malicioso a su registro o interceptado la descarga a su host.
- Docker Content Trust es un mecanismo para firmar y verificar imágenes.
- Los creadores de imágenes pueden firmar sus imágenes para demostrar que son de su autoría; los consumidores que extraen imágenes pueden verificar la confianza comparando la firma pública de la imagen.

5. Lint Dockerfiles

- Los comprobadores de código como Hadolint comprueban las instrucciones de tu Dockerfile y señalan cualquier problema que contravenga las mejores prácticas.

- Corregir los problemas detectados antes de compilar ayudará a garantizar que tus imágenes sean seguras y fiables. Este es otro proceso que puede incorporar a los procesos de CI.