Boletín de alerta

Boletín Nro.:
Fecha de publicación: 12/08/2026
Tema: Alerta 2026-87 Vulnerabilidad CopyEscape en Docker
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- moby/go-archive anteriores a 0.3.0.
- Docker Desktop anterior a 4.86.0.
- Docker Sandboxes anteriores a 0.38.0 para la funcionalidad sbx cp de copia hacia el host.

Descripción

Se ha divulgado una vulnerabilidad de seguridad identificada como **CVE-2026-17106**, denominada **CopyEscape**, que afecta al mecanismo utilizado por Docker para copiar archivos desde un contenedor hacia el sistema host mediante el comando docker cp.

La vulnerabilidad fue descubierta por investigadores de **Imperva Red Team** y permite que un contenedor controlado por un atacante manipule el proceso de copia de archivos para provocar que Docker escriba o sobrescriba archivos fuera del directorio seleccionado originalmente por el usuario.

La falla se produce dentro del proceso de extracción de archivos TAR utilizado por Docker. Cuando se ejecuta una operación de copia desde un contenedor, el Docker daemon genera un archivo TAR basado en el sistema de archivos del contenedor y lo envía al Docker CLI, el cual posteriormente lo extrae en el sistema host.

CopyEscape combina principalmente dos condiciones:

- Una condición de carrera en el sistema de archivos del contenedor que permite generar un archivo TAR inconsistente.
- Una falla durante la extracción que permite seguir enlaces simbólicos hacia ubicaciones externas al directorio de destino.

Como resultado, un contenedor malicioso puede provocar que el Docker CLI escriba archivos en ubicaciones arbitrarias del sistema host utilizando los privilegios del usuario o proceso que ejecutó docker cp.

Solución

Se recomienda a los administradores realizar las siguientes acciones:

- Actualizar **Docker Engine y Docker CLI a 29.7.2 o superior**.
- Actualizar **Docker Desktop a 4.86.0 o superior**.
- Actualizar **Docker Sandboxes a 0.38.0 o superior**.
- Asegurarse de utilizar moby/go-archive 0.3.0 o posterior cuando sea utilizado directamente por aplicaciones internas.
- Actualizar Docker en estaciones de trabajo de desarrollo.
- Priorizar runners CI/CD que ejecuten operaciones docker cp.
- Revisar automatizaciones que ejecuten Docker mediante sudo o como usuario root.
- Aplicar el principio de mínimo privilegio a los usuarios que ejecutan Docker CLI.
- Evitar utilizar sudo docker cp salvo que sea estrictamente necesario.
- No copiar archivos desde contenedores no confiables o comprometidos directamente hacia sistemas sensibles.

Información adicional:

- **Imperva Threat Research – CopyEscape: Taking Over Docker Hosts with docker cp**
- **CVE Program – CVE-2026-17106**
- **Docker Desktop Release Notes**
- **Docker Engine Release Notes**
- **Docker Sandboxes Release Notes**