Boletín de alerta

Boletín Nro.: 95
Fecha de publicación: 29/10/2025
Tema: Alerta 2025-95 Vulnerabilidad en Docker Compose
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Docker Compose versión < v2.40.2

Descripción

Se ha reportado una vulnerabilidad en la herramienta de Desarrollo y DevOps llamada Docker Compose, la cual permitía a los atacantes eludir el directorio de caché de Compose y escribir archivos arbitrarios en el sistema anfitrión, simplemente engañando al usuario para que hiciera referencia a un artefacto remoto malicioso. Se identificó la vulnerabilidad como CVE-2025-62725, con una gravedad alta (CVSS 8.9).

Algunas imágenes/artefactos "Compose" publicados en registries OCI pueden incluir metadatos con rutas de archivos. Docker Compose tomaba esas rutas tal cual y las combinaba con su caché local. Con rutas maliciosas (por ejemplo, usando ../ o rutas absolutas), un atacante podía "salirse" del directorio de caché y hacer que Compose escribiera/sobrescribiera archivos en cualquier ubicación del sistema del usuario.

El problema podía explotarse incluso si solo ejecutabas comandos que no deberían modificar nada, como **docker compose config** o **docker compose ps**.

Ya existen varios PoC que podrían acelerar la creación de exploits. Esta vulnerabilidad podría ser eventualmente utilizadas en ataques de cadenas de suministros (Supply Chain Attack) principalmente en ambientes de desarrollo de software y/o ambientes productivos.

Solución:

Actualiza a Docker Compose v2.40.2 o posterior.

https://docs.docker.com/compose/install

Información adicional:

- https://github.com/docker/compose/security/advisories/GHSA-gv8h-7v7w-r22q
- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2025-62725

- https://bugzilla.redhat.com/show_bug.cgi?id=2406643