Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

¡ALERTA! DOCKER LANZA UN PARCHE DE EMERGENCIA PARA UNA VULNERABILIDAD CRÍTICA DE ESCAPE DE CONTENEDORES

25/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Recientemente, Docker corrigió una falla de alta importancia en Docker Desktop para Windows y macOS, identificada con el ID CVE-2025-9074 y con una puntuación CVSS de 9.3.

¡ALERTA! DOCKER LANZA UN PARCHE DE EMERGENCIA PARA UNA VULNERABILIDAD CRÍTICA DE ESCAPE DE CONTENEDORES

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_25_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	25/08/2025
Es día cero (0 day):	No

RESUMEN

Recientemente, Docker corrigió una falla de alta importancia en Docker Desktop para Windows y macOS, identificada con el ID CVE-2025-9074 y con una puntuación CVSS de 9.3.

La vulnerabilidad permitía que un contenedor malicioso escapara de su aislamiento y accediera al sistema host sin necesidad de que el socket de Docker estuviera montado, lo que representaba un riesgo significativo.

¿Cómo funcionaba la vulnerabilidad?

El problema radica en que, normalmente, Docker Desktop (en Windows y macOS) crea una máquina virtual ligera donde se ejecuta el motor de Docker (Docker Engine). Los contenedores deberían estar aislados y no tener acceso al sistema host.

Sin embargo, debido a un problema de diseño, Docker Desktop exponía una API interna sin autenticación en la dirección 192.168.65.7:2375. Esta API es la misma que los administradores usan para comunicarse con el motor de Docker y controlar los contenedores.

El atacante necesitaba que el usuario ejecutara su imagen de Docker (por ejemplo, descargando un contenedor desde Docker Hub sin revisar la fuente). Luego, desde dentro del contenedor, el atacante abría una conexión a 192.168.65.7:2375. Como no había autenticación, el acceso era directo.

Desde ese momento, el contenedor podía usar los comandos de la API para:

- Crear otros contenedores.
- Mostrar carpetas del host.
- Ejecutar procesos con privilegios elevados.

Al manipular los archivos del sistema operativo anfitrión, el atacante lograba romper el aislamiento de Docker. En Windows, incluso podía ejecutar código con privilegios administrativos. En macOS, aunque la sandbox pide autorización para montar carpetas del usuario, el atacante aún podía manipular configuraciones sensibles de Docker Desktop.

Versiones afectadas y corregidas

- Versiones afectadas: Todas las versiones anteriores a la 4.37.0.
- Versiones corregidas: Docker Desktop 4.37.0 y posteriores.

Es importante mencionar que, en Linux, este fallo no se presentaba porque el motor de Docker usa named pipes o Unix sockets en lugar de exponer un socket TCP abierto en esa dirección.

RECOMENDACIONES

- Limita el número de usuarios que tienen acceso al grupo docker.
- Instala la versión 4.37.0 o superior lo antes posible.
- No expongas el puerto 2375 sin autenticación ni cifrado.
- Si necesitas usar este puerto, habilita TLS/SSL para proteger la conexión.

NOTICIA COMPLETA

https://devel.group/blog/alerta-docker-lanza-un-parche-de-emergencia-para-una-vulnerabilidad-critica-de-escape-de-contenedores/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group