| | |
|---|---|
| **Alerta Id** | 0019 |
| **Fecha del reporte** | 08/28/2025 |
| **Entidad** | Todas las entidades del ecosistema digital |
| **Título** | Vulnerabilidad crítica en Docker Desktop (CVE-2025-9074) permite ejecución de comandos privilegiados desde contenedores |
| **Herramienta de detección** | Avisos de seguridad de INCIBE y DockerFortirecon |
| **Activo involucrado** | Docker Desktop para Windows y MacOS – versiones anteriores a la 4.44.3 |
| **Tipo de alerta** | Vulnerabilidad crítica con posibilidad de explotación local y remota (SSRF / contenedores maliciosos) |
| **Nivel de riesgo** | Crítico |

## Objetivo

Alertar a todas las entidades del ecosistema digital sobre la vulnerabilidad crítica CVE-2025-9074 en Docker Desktop para Windows y MacOS, que permite a un atacante ejecutar comandos con privilegios a través del socket de la API del motor Docker, comprometiendo contenedores y, en algunos casos, el sistema host

## Descripción

El 26 de agosto de 2025, el Instituto Nacional de Ciberseguridad (INCIBE) publicó el aviso INCIBE-2025-0456, confirmando una vulnerabilidad crítica en Docker Desktop para Windows y MacOS.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

La vulnerabilidad permite a los contenedores acceder al Docker Engine a través de la subred por defecto `192.168.65.7:2375`, sin necesidad de autenticación. Un atacante podría:

- Crear, eliminar o modificar contenedores.
- Montar volúmenes críticos (por ejemplo, bases de datos).
- Manipular el sistema de archivos del host.

En Windows, debido al uso de WSL2, es posible montar el sistema de archivos con privilegios administrativos, facilitando la escalada de privilegios y comprometiendo el host.
En MacOS, el impacto es menor por requerir permisos adicionales para acceder al sistema de archivos, aunque el atacante mantiene control total de los contenedores y de la aplicación Docker.
En Linux, la vulnerabilidad no se presenta ya que se utiliza un socket local seguro en lugar de TCP.

La vulnerabilidad fue corregida en la versión 4.44.3 de Docker Desktop, publicada el 21 de agosto de 2025.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570


## Impacto

- **Ejecución de comandos con privilegios** en la API del motor Docker.
- **Control total de contenedores** en ejecución.
- **Acceso no autorizado a archivos sensibles del host** (Windows con mayor impacto que MacOS).
- **Riesgo de escalada de privilegios a administrador del host en Windows**.
- Posible **uso en cadenas de explotación vía SSRF** en aplicaciones expuestas.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

## Recomendaciones de mitigación

1. **Actualizar Docker Desktop** a la versión **4.44.3 o superior**, disponible en el portal oficial de Docker.

2. **Verificar entornos de desarrollo** en Windows y MacOS que utilicen contenedores de terceros o código no confiable.

3. **Evitar exponer el socket Docker en interfaces de red** sin autenticación ni TLS.

4. **Monitorizar actividad inusual en contenedores**, como creación o eliminación no autorizada de imágenes/volúmenes.

5. Implementar **segregación de entornos de desarrollo y producción**, minimizando el uso de Docker Desktop en sistemas críticos.

## Fuentes


- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/ejecucion-de-comandos-en-aplicacion-de-escritorio-de-docker-para-windows-y-macos
- https://pvotal.tech/breaking-dockers-isolation-using-docker-cve-2025-9074/
- https://docs.docker.com/desktop/release-notes/#security




CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570