Docker ha emitido una advertencia sobre una falla crítica que afecta a ciertas versiones de Docker Engine, la cual podría permitir a un atacante eludir los plugins de autorización (AuthZ) en circunstancias específicas.

Identificada como CVE-2024-41110, la vulnerabilidad de omisión y escalada de privilegios tiene una puntuación CVSS de 10.0, lo que indica la máxima gravedad.

> *«Un atacante podría explotar una omisión utilizando una solicitud API con Content-Length establecido en 0, haciendo que el demonio de Docker reenvíe la solicitud sin el cuerpo al plugin AuthZ, el cual podría aprobar la solicitud incorrectamente»,* dijeron los mantenedores del Proyecto Moby en un aviso.

Docker señaló que el problema es una regresión, ya que fue descubierto originalmente en 2018 y solucionado en Docker Engine v18.09.1 en enero de 2019, pero nunca se trasladó a las versiones posteriores (19.03 y posteriores).

El problema se ha solucionado en las versiones 23.0.14 y 27.1.0 a partir del 23 de julio de 2024, después de ser identificado en abril de 2024. Las siguientes versiones de Docker Engine están afectadas, suponiendo que se utiliza AuthZ para tomar decisiones de control de acceso:

- <= v19.03.15
- <= v20.10.27
- <= v23.0.14
- <= v24.0.9
- <= v25.0.5
- <= v26.0.2
- <= v26.1.4
- <= v27.0.3
- <= v27.1.0

> *«Los usuarios de Docker Engine v19.03.x y versiones posteriores que no dependen de los plugins de autorización para tomar decisiones de control de acceso, y los usuarios de todas las versiones de Mirantis Container Runtime, no son vulnerables»,* dijo Gabriela Georgieva de Docker.
>
> *«Los usuarios de productos comerciales de Docker y la infraestructura interna que no dependen de los plugins AuthZ no están afectados.»*

También afecta a Docker Desktop hasta las versiones 4.32.0, aunque la empresa señaló que la probabilidad de explotación es limitada y requiere acceso a la API de Docker, lo que significa que un atacante ya debe tener acceso local al host. Se espera que una solución se incluya en una próxima versión (versión 4.33).

> *«La configuración predeterminada de Docker Desktop no incluye plugins AuthZ. La escalada de privilegios se limita a la máquina virtual de Docker Desktop, no al host subyacente»,* señaló Georgieva.

Aunque Docker no menciona que CVE-2024-41110 haya sido explotada en el entorno real, es esencial que los usuarios actualicen sus instalaciones a la última versión para mitigar posibles amenazas.

A principios de este año, Docker tomó medidas para corregir un conjunto de fallas denominadas Leaky Vessels, que podrían permitir a un atacante obtener acceso no autorizado al sistema de archivos del host y escapar del contenedor.

> *«A medida que los servicios en la nube ganan popularidad, también lo hace el uso de contenedores, los cuales se han convertido en una parte integrada de la infraestructura en la nube. Aunque los contenedores ofrecen muchas ventajas,*

> *también son susceptibles a técnicas de ataque como las fugas de contenedores»,* dijo Palo Alto Networks Unit 42 en un informe publicado la semana pasada.
>
> *«Compartiendo el mismo kernel y a menudo careciendo de un aislamiento completo del modo de usuario del host, los contenedores son susceptibles a diversas técnicas empleadas por atacantes que buscan escapar de los confines de un entorno de contenedor.»*