Se ha revelado una grave vulnerabilidad de seguridad en el NVIDIA Container Toolkit que, si es explotada con éxito, podría permitir a los atacantes salir del entorno limitado del contenedor y obtener acceso total al servidor anfitrión.

La vulnerabilidad, conocida como CVE-2024-0132, tiene una calificación CVSS de 9.0 sobre 10.0. El problema ha sido solucionado en la versión v1.16.2 del NVIDIA Container Toolkit y en la versión 24.6.2 del NVIDIA GPU Operator.

> *«Las versiones 1.16.1 o anteriores del NVIDIA Container Toolkit contienen una vulnerabilidad de tipo 'Time-of-Check Time-of-Use' (TOCTOU) cuando se utilizan con la configuración predeterminada. Una imagen de contenedor manipulada podría lograr acceso al sistema de archivos del servidor anfitrión»,* explicó NVIDIA en un aviso de seguridad.
>
> *«Una explotación exitosa de esta vulnerabilidad podría resultar en la ejecución de código, denegación de servicio, escalada de privilegios, revelación de información y alteración de datos».*

El problema afecta a todas las versiones del NVIDIA Container Toolkit hasta la v1.16.1, así como al Nvidia GPU Operator hasta la versión 24.6.1. No obstante, no impacta los casos en los que se utiliza la Interfaz de Dispositivo de Contenedor (CDI).

La firma de seguridad en la nube Wiz, que descubrió y notificó esta vulnerabilidad a NVIDIA el 1 de septiembre de 2024, señaló que un atacante con control sobre las imágenes de los contenedores gestionados por el Toolkit podría llevar a cabo un escape del contenedor y obtener acceso completo al servidor.

En un escenario de ataque hipotético, un actor malicioso podría crear una imagen de contenedor malintencionada que, al ejecutarse en la plataforma objetivo, ya sea de forma

directa o indirecta, le otorgaría control total sobre el sistema de archivos.

Esto podría ocurrir en un ataque a la cadena de suministro, donde la víctima es engañada para ejecutar la imagen maliciosa, o a través de servicios que permiten compartir recursos de GPU.

> *«Con este acceso, el atacante podría alcanzar los sockets Unix del entorno de ejecución de contenedores (docker.sock/containerd.sock)»*, indicaron los investigadores de seguridad Shir Tamari, Ronen Shustin y Andres Riancho.
>
> *«Estos sockets podrían ser utilizados para ejecutar comandos arbitrarios en el sistema anfitrión con privilegios de root, lo que les daría control completo sobre la máquina».*

El problema representa un riesgo importante para entornos orquestados y multitenant, ya que permitiría a un atacante escapar del contenedor y acceder a los datos y secretos de otras aplicaciones en el mismo nodo o incluso en el mismo clúster.

Los detalles técnicos del ataque se han mantenido en secreto por ahora para evitar que se explote la vulnerabilidad. Se recomienda encarecidamente a los usuarios que apliquen los parches correspondientes para protegerse de posibles amenazas.

> *«Aunque los riesgos de seguridad en IA suelen enfocarse en ataques futuristas basados en inteligencia artificial, las vulnerabilidades de infraestructura 'tradicionales' en el creciente ecosistema de tecnología de IA siguen siendo una amenaza inmediata que los equipos de seguridad deben priorizar»,* comentaron los investigadores.