El investigador de seguridad cibernética, Paul Litvak, reveló una vulnerabilidad sin parchear en Microsoft Azure Functions, que un atacante podría utilizar para escalar privilegios y escapar del contenedor Docker utilizado para alojarlos.

Los hallazgos forman parte de las investigaciones de Intezer Labs acerca de la infraestructura informática de Azure.

Después de la divulgación a Microsoft, la compañía *«determinó que la vulnerabilidad no tiene ningún impacto en la seguridad de los usuarios de la función, ya que el host en sí todavía está protegido por otro límite de defensa contra la posición elevada que alcanzamos en el host contenedor».*

Azure Functions, análoga a Amazon AWS Lambda, es una solución sin servidor que permite a los usuarios ejecutar código desencadenado por eventos sin necesidad de aprovisionar o administrar la infraestructura explícitamente, y al mismo tiempo, hacer posible escalar y asignar recursos y procesamiento según la demanda.

Al incorporar Docker en la combinación, los desarrolladores pueden implementar y ejecutar fácilmente Azure Functions en la nube o en las instalaciones.

Debido a que el código desencadenante es un evento (por ejemplo, una solicitud HTTP) que está configurado para llamar a una función de Azure, los investigadores primero crearon un desencadenador HTTP para afianzarse en el contenedor de funciones, usándolo para encontrar sockets que pertenecen a procesos con privilegios de root.

A partir de esto, se identificó que uno de esos procesos privilegiados asociados con un binario *«Mesh»* contenía una falla que podría explotarse para otorgar permisos al usuario de la aplicación que ejecuta los permisos de la raíz de la función anterior.

Aunque el binario Mesh en sí mismo tenía poca o ninguna documentación para explicar su propósito, los investigadores de Intezer encontraron referencias a él en una imagen pública de Docker, que utilizaron para realizar ingeniería inversa y lograr una escalada de privilegios.

Finalmente, se abusó de los privilegios extendidos asignados al contenedor para escapar del contenedor Docker y ejecutar un comando arbitrario en el host.

Intezer también lanzó un código de explotación de prueba de concepto (PoC) en GitHub para probar el entorno de host de Docker.

> *«Ejemplos como este subrayan que las vulnerabilidades a veces están fuera del control del usuario de la nube. Los atacantes pueden encontrar una forma de entrar por medio de software vulnerable de terceros»,* dijeron los investigadores.
>
> *«Es fundamental que cuente con medidas de protección para detectar y terminar cuando el atacante ejecuta código no autorizado en su entorno de producción. Esta mentalidad de Confianza Cero se hace eco incluso en Microsoft».*