Los investigadores de seguridad cibernética revelaron una nueva vulnerabilidad grave de Oracle Cloud Infrastructure (OCI) que los usuarios podrían explotar para acceder a los discos virtuales de otros clientes de Oracle.

> *«Cada disco virtual en la nube de Oracle tiene un identificador único llamado OCID. Este identificador no se considera secreto y las organizaciones no lo tratan como tal»,* dijo Shir Tamari, jefe de investigación de Wiz.

> *«Dado el OCID del disco de una víctima que actualmente no está conectado a un servidor activo o configurado como compatible, un atacante podría 'conectarse a él' y obtener lectura/escritura sobre él».*

La compañía de seguridad en la nube, que denominó la vulnerabilidad de aislamiento de inquilinos «AttachMe«, dijo que Oracle solucionó el problema dentro de las 24 horas posteriores a la divulgación responsable el 9 de junio de 2022.

En esencia, la vulnerabilidad se basa en el hecho de que un disco podría conectarse a una instancia de cómputo en otra cuenta por medio del Oracle Cloud Identifier (OCID) sin ninguna autorización explícita.

Esto significa que un atacante en posesión del OCID podría haberse aprovechado de AttachMe para acceder a cualquier volumen de almacenamiento, lo que daría como resultado la exposición de datos, la exfiltración o, peor aún, la alteración de los volúmenes de arranque para lograr la ejecución del código.

Además de conocer el OCID del volumen objetivo, otro requisito previo para llevar a cabo el ataque es que la instancia del adversario debe estar en el mismo dominio de disponibilidad (AD) que el objetivo.

> *«La validación insuficiente de los permisos de los usuarios es una clase de error común entre los proveedores de servicios en la nube. La mejor forma de identificar dichos problemas es realizar revisiones rigurosas de código y pruebas exhaustivas para cada API sensible en la etapa de desarrollo»,* dijo el investigador de Wiz, Elad Gabay.

Los hallazgos llegan casi cinco meses después de que Microsoft abordara un par de problemas con Azure Database for PostgreSQL Flexible Server, que podrían resultar en el acceso no autorizado a la base de datos entre cuentas en una región.