Microsoft reveló el jueves que abordó vulnerabilidades en Azure Database for PostgreSQL Flexible Server, que podrían resultar en el acceso no autorizado a la base de datos entre cuentas en una región.

> *«Al explotar un error de permisos elevados en el proceso de autenticación del servidor flexible para un usuario de replicación, un usuario malicioso podría aprovechar una expresión regular anclada incorrectamente para evitar la autenticación y obtener acceso a las bases de datos de otros clientes»,* dijo Microsoft Security Response Center (MSRC).

La compañía de seguridad en la nube Wiz, con sede en Nueva York, descubrió las vulnerabilidades y denominó a la cadena de exploits como «ExtraReplica«. Microsoft dijo que mitigó el error dentro de las 48 horas posteriores a la divulgación el 13 de enero de 2022.

Específicamente, se relaciona con un caso de escalada de privilegios en el motor de Azure PostgreSQL para obtener la ejecución de código y una omisión de autenticación entre cuentas mediante un certificado falsificado, lo que permite a un atacante crear una base de datos en la región de Azure del objetivo y filtrar información confidencial.

En otras palabras, la explotación exitosa de las vulnerabilidades críticas podría haber permitido que un adversario obtuviera acceso de lectura no autorizado a las bases de datos PostgreSQL de otros clientes, eludiendo de este modo el aislamiento de inquilinos.

Wiz rastreó la escalada de privilegios a un error derivado de las modificaciones introducidas en el motor PostgreSQL para fortalecer su modelo de privilegios y agregar nuevas funciones. El nombre ExtraReplica proviene del hecho de que el exploit aprovecha una función PostgreSQL que permite copiar datos de la base de datos de un servidor a otro, es decir, «replicar» la base de datos.

Microsoft dijo que la vulnerabilidad de seguridad afectaba a las instancias de PostgreSQL Flexible Server implementadas mediante la opción de red de acceso público, pero enfatizó

que no encontró evidencia de que la falla se explotara activamente y que no se accedió a los datos del cliente.

> *«No se requiere ninguna acción por parte de los clientes. Para minimizar aún más la exposición, recomendamos que los clientes habiliten el acceso a la red privada al configurar sus instancias de servidor flexible»,* dijo MSRC.