La compañía de seguridad de infraestructura en la nube Wiz, reveló este jueves los detalles de una vulnerabilidad de la base de datos de Azure Cosmos, ya corregida, que podría haber sido potencialmente explotada para otorgar a cualquier usuario de Azure acceso de administrador completo a las instancias de la base de datos de otros clientes sin ninguna autorización.

La vulnerabilidad, que otorga privilegios de lectura, escritura y eliminación, se ha denominado «ChaosDB«, y los investigadores de Wiz afirman que *«la vulnerabilidad tiene un exploit trivial que no requiere ningún acceso previo al entorno de destino y afecta a miles de organizaciones, incluidas numerosas empresas de Fortune 500».*

Cosmos DB es la base de datos NoSQL patentada de Microsoft que se anuncia como *«un servicio completamente administrado que le quita de las manos la administración de la base de datos con administración automática, actualizaciones y parches».*

El equipo de investigación de Wiz informó el problema a Microsoft el 12 de agosto, luego de lo cual, el fabricante de Windows tomó medidas para mitigar el problema dentro de las 48 horas posteriores a la divulgación responsable, además de otorgar una recompensa de 40 mil dólares a los buscadores el 17 de agosto.

> *«No tenemos ninguna indicación de que entidades externas fuera del investigador tuvieran acceso a la clave principal de lectura y escritura asociada con sus cuentas de Azure Cosmos DB. Además, no tenemos conocimiento de ningún acceso a datos debido a esta vulnerabilidad. Las cuentas de Azure Cosmos DB con una vNET o un firewall habilitado están protegidas por mecanismos de seguridad adicionales que evitan el riesgo de acceso no autorizado»*, dijo Microsoft.

El exploit identificado por Wiz, se refiere a una cadena de vulnerabilidades en la función Jupyter Notebook de Cosmos DB, lo que permite a un atacante obtener las credenciales correspondientes a la cuenta de Cosmos DB de destino, incluyendo la clave principal, que proporciona acceso a los recursos administrativos para la cuenta de la base de datos.

> *«Con estas credenciales, es posible ver, modificar y eliminar datos en la cuenta de Cosmos DB de destino a través de múltiples canales»,* dijeron los investigadores.

Como consecuencia de esto, cualquier activo de Cosmos DB que tenga habilitada la función Jupyter Notebook se verá potencialmente afectado.

Aunque Microsoft notificó a más del 30% de los clientes de Cosmos DB sobre la posible violación de seguridad, Wiz espera que el número real sea mucho mayor, debido a que la vulnerabilidad ha sido explotable por meses.

> *«Cada cliente de Cosmos DB debe asumir que ha estado expuesto. También recomendamos revisar toda la actividad pasada en su cuenta de Cosmos DB»,* dijeron los investigadores.

Además, Microsoft también insta a sus clientes a regenerar sus claves primarias de Cosmos DB para mitigar cualquier riesgo que surja de la falla.