Microsoft dijo este martes que abordó una vulnerabilidad de omisión de autenticación en Jupyter Notebooks para Azure Cosmos DB, que permitía el acceso completo de lectura y escritura a las bases de datos.

La compañía dijo que el problema se presentó el 12 de agosto de 2022 y se solucionó en todo el mundo el 6 de octubre de 2022, dos días después de la divulgación responsable de Orca Security, que denominó la falla como CosMiss.

> *«En resumen, si un atacante tuviera conocimiento del 'forwardingId' de una computadora portátil, que es el UUID del espacio de trabajo de la computadora portátil, habría tenido permisos completos en la computadora portátil sin tener que autenticarse, incluid el acceso de lectura y escritura, y la capacidad de modificar el sistema de archivos del contenedor que ejecuta el portátil»,* dijeron los investigadores Lidor Ben Dhitrit y Roee Sagi.

En última instancia, esta modificación del contenedor podría allanar el camino para obtener la ejecución remota de código en el contenedor de Notebook al sobrescribir un archivo de Python asociado con Coscmos DB Explorer para generar un shell inverso.

Sin embargo, la explotación exitosa de la vulnerabilidad requiere que el atacante esté en posesión del identificador de reenvío único de 128 bits y que se use dentro de una ventana de una hora, después de lo cual el cuaderno temporal se elimina de forma automática.

> *«La vulnerabilidad, incluso con el conocimiento del forwardingId, no permitía ejecutar cuadernos, guardar automáticamente cuadernos en el repositorio de GitHub conectado (opcional) de la víctima o acceder a datos en la cuenta de Azure Cosmos DB»*, dijo Redmond.

Microsoft dijo en su propio aviso que no identificó evidencia de actividad maliciosa y agregó

que no se requiere ninguna acción por parte de los clientes. También describió el problema como *«difícil de explotar»* debido a la aleatoriedad del forwardingID de 128 bits y su vida útil limitada.

> *«Los clientes que no usan portátiles Jupyter (el 99.8% de los clientes de Azure Cosmos DB NO usan portátiles Jupyter) no eran susceptibles a esta vulnerabilidad»,* agregó.