Investigadores de seguridad cibernética revelaron hoy los detalles de una vulnerabilidad de memoria en la familia de productos de administración de datos Db2 de IBM, que podría permitir que un atacante local acceda a datos confidenciales e incluso, realice ataques de denegación de servicios.

La vulnerabilidad, rastreada como CVE-2020-4414, afecta a las ediciones IBM DB2 v9.7, v10.1, v10.5, v11.1 y v11.5 en todas las plataformas, y es causada por un uso inadecuado de la memoria compartida.

Al enviar una solicitud especialmente diseñada, un atacante podría aprovechar la vulnerabilidad para obtener información confidencial o provocar una denegación de servicio, según el equipo de investigación y seguridad de Trustware Spider Labs, que descubrió el problema.

> *«Los desarrolladores se olvidaron de poner protecciones de memoria explícitas alrededor de la memoria compartida utilizada por la función de rastreo de DB2. Esto permite que cualquier usuario local lea y escriba acceso a esa área de memoria. A su vez, esto permite acceder a datos críticamente sensibles, así como la capacidad de cambiar cómo funciona el subsistema de rastreo, lo que resulta en una condición de denegación de servicio en la base de datos»,* dijo Martin Rakhmanov.

IBM lanzó un parche el 30 de junio de 2020 para corregir la vulnerabilidad.

El error se debe al uso inseguro de la memoria compartida que la utilidad de seguimiento de DB2 emplea para intercambiar información con el sistema operativo subyacente en el sistema.

La utilidad de rastreo de DB2 se utiliza para registrar datos y eventos de DB2, incluidos los informes de información del sistema de DB2, la recopilación de datos necesarios para el análisis y el ajuste del rendimiento y la captura de pistas de auditoría de acceso a datos con fines de seguridad.

Debido a que la memoria compartida almacena información confidencial, un atacante con acceso al sistema podría crear una aplicación maliciosa para sobrescribir la memoria con datos falsos dedicados a rastrear datos.

> *«Esto significa que un usuario local sin privilegios puede abusar de esto para causar una condición de denegación de servicio simplemente escribiendo datos incorrectos en la sección de memoria»*, dijo el investigador.

Además, un proceso con pocos privilegios que se ejecute en el mismo equipo que la base de datos DB2 podría alterar el rastreo de DB2 y capturar datos confidenciales, además de utilizar la información para llevar a cabo otros ataques.