Se ha revelado una vulnerabilidad de alta gravedad en MongoDB que podría permitir a usuarios no autenticados leer memoria del *heap* que no ha sido inicializada.

La falla, identificada como CVE-2025-14847 (puntuación CVSS: 8.7), se describe como un problema derivado del manejo incorrecto de inconsistencias en los parámetros de longitud. Este tipo de error ocurre cuando un programa no gestiona adecuadamente situaciones en las que el campo de longitud no coincide con el tamaño real de los datos asociados.

"Los campos de longitud inconsistentes en los encabezados de protocolo comprimidos con Zlib pueden permitir que un cliente no autenticado lea memoria del heap no inicializada", según la descripción de la vulnerabilidad publicada en CVE.org.

La falla afecta a las siguientes versiones de la base de datos:

- MongoDB 8.2.0 a 8.2.3
- MongoDB 8.0.0 a 8.0.16
- MongoDB 7.0.0 a 7.0.26
- MongoDB 6.0.0 a 6.0.26
- MongoDB 5.0.0 a 5.0.31
- MongoDB 4.4.0 a 4.4.29
- Todas las versiones de MongoDB Server v4.2
- Todas las versiones de MongoDB Server v4.0
- Todas las versiones de MongoDB Server v3.6

El problema fue corregido en las versiones 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32 y 4.4.30 de MongoDB.

"Una explotación del lado del cliente de la implementación zlib del servidor puede devolver memoria del heap no inicializada sin necesidad de autenticarse en el servidor", indicó MongoDB. *"Recomendamos encarecidamente actualizar a una versión corregida lo antes posible."*

Si no es posible realizar la actualización de inmediato, se aconseja deshabilitar la compresión zlib en el servidor MongoDB, iniciando *mongod* o *mongos* con las opciones networkMessageCompressors o net.compression.compressors, asegurándose de excluir explícitamente zlib. Las otras opciones de compresión compatibles con MongoDB son snappy y zstd.

"CVE-2025-14847 permite que un atacante remoto no autenticado provoque una condición en la que el servidor MongoDB pueda devolver memoria no inicializada de su heap", señaló OP Innovate. *"Esto podría derivar en la divulgación de datos sensibles en memoria, como información sobre el estado interno, punteros u otros datos que podrían facilitar una explotación adicional."*