# Boletín de alerta

**Boletín Nro.:**
**Fecha de publicación:** 27/03/2026
**Tema:** Alerta 2026-29 Vulnerabilidad crítica en MongoDB
**Traffic Light Protocol (TLP):** Amber

## Producto(s) afectado(s):

- MongoDB Server 8.2.x (anteriores a 8.2.6)
- MongoDB Server 8.0.x (anteriores a 8.0.20)
- MongoDB Server 7.0.x (anteriores a 7.0.31)

## Descripción

Recientemente se descubrió una vulnerabilidad crítica en MongoDB. **MongoDB** es un sistema de base de datos NoSQL ampliamente utilizado para almacenar grandes volúmenes de información de forma flexible, especialmente en aplicaciones web y servicios modernos.

La vulnerabilidad **CVE-2026-4148 con una puntuación de 8.7 en CVSS v4.0** en MongoDB se origina por un error en la gestión de memoria conocido como *"uso después de liberar memoria"* (*use-after-free*).

Esto ocurre cuando el sistema sigue utilizando un espacio de memoria que ya fue liberado, lo que puede provocar comportamientos inesperados o inseguros.

En este caso, el problema se presenta en clústeres fragmentados (sharded clusters) cuando se ejecutan consultas de agregación complejas como $lookup o $graphLookup. Estas consultas, si están especialmente diseñadas, pueden hacer que MongoDB utilice referencias a memoria que ya no es válida.

El error está relacionado con la forma en que MongoDB maneja y duplica (clona) partes internas de las consultas. Durante este proceso, algunas referencias no se actualizan correctamente, quedando "apuntando" a memoria que ya fue liberada.

Esta vulnerabilidad puede afectar directamente la **disponibilidad, confidencialidad e integridad** de la información almacenada en MongoDB. Un atacante con acceso autenticado podría provocar interrupciones en el servicio (caídas o lentitud), así como acceder o manipular datos sensibles dentro de la base de datos.

## Solución y mitigaciones:

- Actualizar MongoDB Server a la versión más reciente disponible

## Información adicional:

- https://www.tenable.com/cve/CVE-2026-4148
- https://jira.mongodb.org/browse/SERVER-119319
- https://www.cert.gov.py/vulnerabilidad-en-productos-mongodb/