# Boletín de alerta

**Boletín Nro.:** 106
**Fecha de publicación:** 24/12/2025
**Tema:** Alerta 2025-106 Vulnerabilidad crítica en MongoDB
**Traffic Light Protocol (TLP):** White

## Producto(s) afectado(s):

Las siguientes ediciones del servidor MongoDB están afectadas:

- **MongoDB 8.2.x** versiones hasta 8.2.2
- **MongoDB 8.0.x** versiones hasta 8.0.16
- **MongoDB 7.0.x** versiones hasta 7.0.26
- **MongoDB 6.0.x** versiones hasta 6.0.26
- **MongoDB 5.0.x** versiones hasta 5.0.31
- **MongoDB 4.4.x** versiones hasta 4.4.29
- **MongoDB 4.2.x** todas las versiones
- **MongoDB 4.0.x** todas las versiones
- **MongoDB 3.6.x** todas las versiones

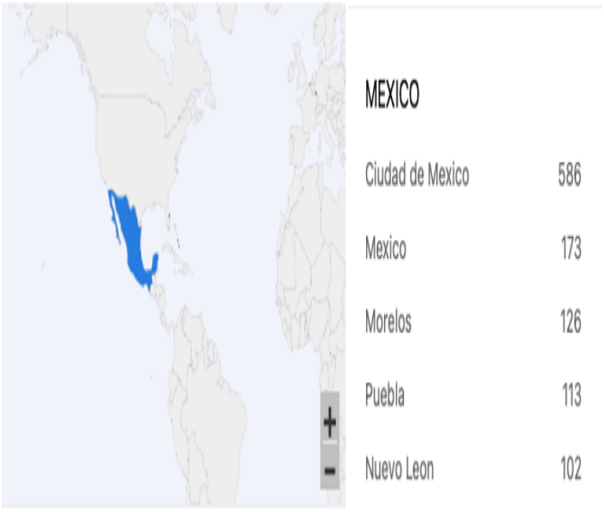
## Descripción

Recientemente, el equipo de seguridad de MongoDB, Inc., ha reportado y publicado la vulnerabilidad **CVE-2025-14847 con score CVSS 3.1 de 7.5**, la cual presenta un **fallo en la gestión de los encabezados de protocolo comprimidos usando zlib** en el servidor MongoDB. Específicamente, la implementación en versiones afectadas **no valida correctamente campos de longitud en dichos encabezados**, lo que permite a clientes remotos y no autenticados provocar la lectura de memoria del montículo (heap) no inicializada.

La explotación de esta vulnerabilidad **no requiere credenciales, privilegios ni interacción del usuario;** un actor con acceso a la red y al puerto de la base de datos puede enviar paquetes especialmente construidos para provocar que la instancia de MongoDB devuelva bloques de memoria arbitraria. Esto genera una divulgación de información sensible (como datos de sesiones, fragmentos de consultas o incluso credenciales en caché) sin afectar la integridad ni la disponibilidad del servicio.

De acuerdo con la base de datos de NVD y múltiples análisis técnicos, el fallo está clasificado bajo CWE-130 (Improper Handling of Length Parameter Inconsistency), lo cual indica una inconsistencia en cómo se manejan los parámetros de longitud dentro de las interfaces de compresión de protocolo.

Según ZoomEye, tan solo **en México se identifican casi 2000 servidores** que utilizan MongoDB, por lo que se recomienda encarecidamente revisar las versiones y de ser posible actualizar lo antes posible a las últimas versiones.




*Servidores con MongoDB en México*

## Mitigaciones y soluciones:

- **Actualizar a versiones parcheadas de MongoDB:**

MongoDB, Inc. ha liberado versiones que corrigen el fallo para cada rama afectada. Se recomienda actualizar a: **8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32, 4.4.30.**

Para más información sobre los parches visita el sitio de MongoDB: **MongoDB Updates**

- **Reducción de exposición de red:**

Hasta que se complete la actualización, restringir el acceso de red a los puertos de MongoDB (27017 por defecto) mediante firewalls, VPN, o segmentación de red, limitando el acceso solo a hosts o rangos de confianza.

- **Deshabilitar zlib (temporal):**

Como medida transitoria, los despliegues pueden arrancar mongod/mongos con opciones que deshabiliten la compresión zlib, sustituyéndola por alternativas como snappy o zstd, o eliminando compresión, reduciendo así la superficie explotable.

## Información adicional:

- **https://nvd.nist.gov/vuln/detail/CVE-2025-14847**
- **https://www.redhotcyber.com/en/post/critical-mongodb-vulnerability-exposed-cve-2025-14847**
- **https://securityonline.info/critical-unauthenticated-mongodb-flaw-leaks-sensitive-data-via-zlib-compression**