NATIONAL CSIRT-CY

CVE-2025-14847 **30/12/2025**

MongoDB "MongoBleed" Vulnerability

Executive Summary

This vulnerability with a CVSS score of 7.5 known by the name “MongoBleed” has been actively exploited in the wild. The flaw exists in MongoDB server zlib network message decompression algorithm. The server does not validate the length of the compressed data before processing. This allows, network-level attackers to extract data of uninitialized server memory. An attacker can send crafted compressed payloads to make MongoDB miscalculate decompressed data length and leak memory contents.

This vulnerability enables information leak, which may be used for reconnaissance, data harvesting, or chaining with other attacks.

This vulnerability is remotely exploitable without authentication, has low attack complexity (easy to exploit) and does not require user interaction.

Affected Versions

- MongoDB 8.2 prior to 8.2.3
- MongoDB 8.0 prior to 8.0.17
- MongoDB 7.0 prior to 7.0.28
- MongoDB 6.0 prior to 6.0.27
- MongoDB 5.0 prior to 5.0.32
- MongoDB 4.4 prior to 4.4.30
- All MongoDB Server 4.2.x versions
- All MongoDB Server 4.0.x versions
- All MongoDB Server 3.6.x versions

Solution

Upgrade MongoDB to one of these versions:

- 8.2.3
- 8.0.17
- 7.0.28
- 6.0.27

- 5.0.32
- 4.4.30

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/130.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-14847

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments