مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Unauthenticated Compression Vulnerability in MongoDB

Tracking #:432318164

Date:23-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability was disclosed in MongoDB, allowing remote attackers to extract uninitialized heap memory from the database server without authentication.

TECHNICAL DETAILS:

An unauthenticated information disclosure vulnerability has been identified in MongoDB Server, tracked as CVE-2025-14847.The flaw exists in MongoDB's zlib compression handling, allowing remote attackers to extract uninitialized heap memory from the database server without authentication. With a CVSS v4 score of 8.7, this vulnerability presents a serious risk to exposed MongoDB instances, potentially leaking sensitive data such as cached credentials, query contents, or other in-memory artifacts.

Vulnerability Details:

- CVE ID: CVE-2025-14847
- Severity: High
- CVSS v4 Score: 8.7
- Attack Vector: Network
- Authentication Required: None
- Impact Type: Information Disclosure / Memory Leak
- Affected Component: MongoDB Server – zlib compression implementation

Affected Version:

- MongoDB 8.2.0 through 8.2.3
- MongoDB 8.0.0 through 8.0.16
- MongoDB 7.0.0 through 7.0.26
- MongoDB 6.0.0 through 6.0.26
- MongoDB 5.0.0 through 5.0.31
- MongoDB 4.4.0 through 4.4.29
- All MongoDB Server v4.2 versions
- All MongoDB Server v4.0 versions
- All MongoDB Server v3.6 versions

Fixed Version:

- MongoDB 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32, or 4.4.30.

RECOMMENDATIONS:

- Upgrade MongoDB Server immediately-Apply the latest patched version applicable to deployment.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://jira.mongodb.org/browse/SERVER-115508