مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-MongoDB

Tracking #:432317028

Date:02-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that MongoDB has disclosed three vulnerabilities affecting multiple server versions, exposing deployments to denial-of-service (DoS) attacks, authentication bypass risks, and crashes in critical components.

TECHNICAL DETAILS:

MongoDB has disclosed three vulnerabilities affecting multiple server versions, exposing deployments to denial-of-service (DoS) attacks, authentication bypass risks, and crashes in critical components.

Vulnerability Details:

1. CVE-2025-3083 (CVSS 7.5): Unauthenticated DoS via Malformed Wire Protocol Messages
Impact: Attackers can crash the mongos router process by sending specially crafted messages, disrupting cluster operations.

Root Cause: Improper validation of MongoDB wire protocol messages.

Affected Versions:
- MongoDB 5.0.x < 5.0.31
- MongoDB 6.0.x < 6.0.20
- MongoDB 7.0.x < 7.0.16

Risk: Exploitation requires no authentication, making it a low-barrier attack vector for disrupting database availability

2. CVE-2025-3084 (CVSS 6.5): explain Command Validation Failure
Impact: Malicious queries exploiting invalid arguments can crash router servers.

Root Cause: The explain command fails to validate specific argument combinations before execution.

Affected Versions:
- MongoDB Server 5.0.x < 5.0.31
- MongoDB Server 6.0.x < 6.0.20
- MongoDB Server 7.0.x < 7.0.16
- MongoDB Server 8.0.x < 8.0.4

Risk: Internal attackers or misconfigured applications could trigger crashes with minimal effort

3. CVE-2025-3085 (CVSS 8.1): TLS Certificate Revocation Bypass
Impact: Revoked intermediate certificates may be accepted, enabling unauthorized access in configurations using MONGODB-X509 or intra-cluster authentication.

Root Cause: Inadequate revocation status checks for intermediate certificates when TLS and CRL validation are enabled.

Affected Versions:

- MongoDB Server 5.0.x < 5.0.31
- MongoDB Server 6.0.x < 6.0.20
- MongoDB Server 7.0.x < 7.0.16
- MongoDB Server 8.0.x < 8.0.4

Risk: Attackers with revoked certificates could bypass authentication controls in targeted environment

RECOMMENDATIONS:

- Apply the latest patches for MongoDB versions 5.0.x, 6.0.x, 7.0.x, and 8.0.x to address these vulnerabilities

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-103152
- https://jira.mongodb.org/browse/SERVER-103153
- https://jira.mongodb.org/browse/SERVER-95445