مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Code Injection Vulnerability in MongoDB Compass

Tracking #:432316035

Date:09-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been identified in MongoDB Compass, a popular graphical user interface (GUI) for managing MongoDB databases.

TECHNICAL DETAILS:

A critical security vulnerability (**CVE-2024-6376**) has been identified in MongoDB Compass, a popular graphical user interface (GUI) for managing MongoDB databases. This vulnerability allows attackers to inject malicious code through insufficient sandboxing in the ejson shell parser used by Compass. Exploitation could result in data breaches, unauthorized system access, and data manipulation.

Vulnerability Details:

- **CVE-2024-6376** | CVSS score: 9.8 – Critical(NIST:NVD)
- MongoDB Compass may be susceptible to code injection due to insufficient sandbox protection settings with the usage of ejson shell parser in Compass' connection handling.

Affected Versions:

- MongoDB Compass versions prior to version 1.42.2

Fixed Version:

- MongoDB Compass version 1.42.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected version to the fixed or latest versions released by MongoDB.

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://nvd.nist.gov/vuln/detail/CVE-2024-6376