

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Critical Vulnerability in MongoDB Tool**  
Tracking #:432316761  
Date:20-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in Mongoose, a widely used MongoDB object modeling tool, impacting millions of applications that rely on it for database interactions.

## TECHNICAL DETAILS:

A critical vulnerability has been discovered in Mongoose, a widely used MongoDB object modeling tool, impacting millions of applications that rely on it for database interactions.

### Vulnerability Overview:

The vulnerability, tracked as CVE-2025-23061, allows attackers to exploit improper handling of nested \$where filters in combination with the populate() method, enabling potential search injection attacks. These attacks could lead to unauthorized access to sensitive data, posing a significant security risk to organizations using affected versions of Mongoose.

- Vulnerability ID: **CVE-2025-23061**
- CVSS Score: 9.0 (**Critical**)
- Affected Versions: Mongoose versions prior to 8.9.5
- Impact: Search injection attacks leading to unauthorized access, data manipulation, or database compromise
- Vulnerable Functionality: Improper handling of \$where filters when used with populate()

### Fixed Version:

- Mongoose version 8.9.5

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to users of Mongoose are strongly advised to upgrade to fixed version or later to resolve the issue.

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://github.com/Automattic/mongoose/releases/tag/8.9.5>