

# MongoDB Mongoose 搜索注入漏洞（CVE-2025-23061）通告

|        |                                      |        |            |
|--------|--------------------------------------|--------|------------|
| ■ 通告编号 | NS-2025-0005                         | ■ 发布日期 | 2025-01-21 |
| ■ 漏洞危害 | 攻击者利用此漏洞，可实现代码注入。                    |        |            |
| ■ TAG  | MongoDB Mongoose、搜索注入、CVE-2025-23061 |        |            |



## 一. 漏洞概述

近日，绿盟科技 CERT 监测到 GitHub 发布安全公告，Mongoose 中修复了一个搜索注入漏洞（CVE-2025-23061），此漏洞为 CVE-2024-53900 的修复不完全；由于 Mongoose 错误地将\$where 过滤器与 populate()方法中的 match 条件一起处理，当同时使用了两者查询时未经身份验证的攻击者可操纵进行搜索注入，从而实现代码注入或未授权的数据库访问。CVSS 评分 9.0，请相关用户尽快采取措施进行防护。

Mongoose 是一个用于在 Node.js 中操作 MongoDB 的对象建模库。它提供了一种更结构化的方式来与 MongoDB 交互，通过定义 Schema（模式）来规范数据结构，并提供了如数据验证、查询构建、中间件等多种功能。

参考链接：

<https://github.com/advisories/GHSA-vg7j-7cwx-8wgw>

## 二. 影响范围

受影响版本

- 8.0.0-rc0 <= MongoDB Mongoose < 8.9.5
- 7.0.0-rc0 <= MongoDB Mongoose < 7.8.4
- MongoDB Mongoose < 6.13.6

不受影响版本

- MongoDB Mongoose >= 8.9.5
- MongoDB Mongoose >= 7.8.4
- MongoDB Mongoose >= 6.13.6

## 三. 漏洞检测

### 3.1 版本检测

相关用户可通过下列命令判断当前使用的 **Mongoose** 版本是否存在安全风险：

```
npm list mongoose
```

## 四. 漏洞防护

目前官方已发布新版本修复了该漏洞，请受影响的用户尽快升级版本进行防护，下载链接：<https://github.com/Automattic/mongoose/releases>

相关用户可使用下列命令升级至对应安全版本：

```
npm install mongoose@latest
```

## 声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。