# Dynamic Analysis Report

## 1. Analysis Environment

The analysis was conducted inside a Docker container under a no-network mode (--network=none),  
using strace, inotify, ss, and ps tools to monitor system calls and runtime behavior.  
Duration: 60 seconds. Entry file: node src/server.js. Environment: Node.js v20.19.5, Network: isolated (no outbound connections).  
  
本次分析在 Docker 容器内禁网模式下执行（--network=none），结合 strace、inotify、ss、ps 等工具进行系统调用与行为监控。  
分析时间约 60 秒，入口程序为 node src/server.js。系统环境：Node.js v20.19.5，网络环境：禁网（拒绝外部连接）。

## 2. Runtime Behavior Overview / 运行期行为概述

During initialization, the program displays startup messages indicating RSA-4096 key generation and server setup.  
It automatically creates a 4096-bit RSA key pair, suggesting built-in encryption support.  
  
程序启动时输出日志显示 RSA-4096 密钥生成与服务器初始化信息，自动生成 4096 位 RSA 密钥对，说明系统具备加密通信设计。

The system then attempts to connect to MongoDB on localhost (127.0.0.1:27017 / ::1:27017), but receives ECONNREFUSED since no MongoDB service exists in the container.  
  
系统随后尝试连接本地 MongoDB (127.0.0.1:27017 / ::1:27017)，但因容器中未部署数据库而触发 ECONNREFUSED 错误。

The connection failure causes the process to terminate prematurely, and no network listeners are active.  
The ss.txt file only contains headers, confirming no open ports.  
  
由于数据库连接失败，程序提前终止，未进入监听阶段。ss.txt 文件仅包含表头，确认无开放端口。

## 3. System Call Analysis

strace logs reveal multiple connect() attempts to 127.0.0.1:27017, file reads of project and Node modules, and normal stdout writes.  
No suspicious execve() or access to sensitive files was detected.  
  
strace 日志显示多次 connect() 调用至 127.0.0.1:27017，读取项目文件与 Node 模块，正常输出 stdout。  
未发现可疑 execve() 调用或访问敏感文件行为。

## 4. Summary Results

|  |  |  |
| --- | --- | --- |
| Check Item / 检查项目 | Result / 结果 | Explanation / 说明 |
| External Connections / 外部网络访问 | None / 无 | All connections target localhost / 所有连接均为本地回环地址 |
| Listening Ports / 监听端口 | None / 无 | No ports opened / 程序未开放端口 |
| File I/O / 文件读写 | Normal / 正常 | No sensitive file accessed / 未访问敏感文件 |
| Process Behavior / 进程行为 | Safe / 安全 | No external command execution / 无外部命令执行 |
| Encryption / 加密行为 | RSA-4096 generated / 自动生成 RSA-4096 | Normal key generation / 正常加密行为 |
| Error Handling / 异常处理 | Weak / 不足 | Crashes on MongoDB failure / MongoDB 连接失败后直接退出 |

## 5. Security Evaluation and Recommendations / 安全评估与改进建议

|  |  |  |  |
| --- | --- | --- | --- |
| Category / 类别 | Finding / 发现 | Severity / 严重性 | Recommendation / 改进建议 |
| Database Dependency / 外部依赖连接 | Relies on MongoDB; may attempt external connection if misconfigured / 程序强依赖 MongoDB，若配置错误可能外连公网 | Medium / 中等 | Restrict DB to local network / 限制数据库访问范围 |
| Error Handling / 异常处理 | Uncaught exception on DB failure / 连接拒绝即抛异常退出 | Low–Medium / 低至中 | Add try-catch and retry limits / 增加异常捕获与重试限制 |
| Key Management / 密钥管理 | RSA key generated dynamically / 动态生成 RSA-4096 | Info / 信息 | Ensure keys not logged / 确保密钥不写入日志 |
| Communication / 通信安全 | Uses RSA encryption / 使用 RSA 加密通信 | Normal / 正常 | Maintain encryption practice / 保持当前机制 |
| Syscalls / 系统调用 | No exec or file injection / 未发现命令执行或植入 | Safe / 安全 | Maintain current isolation / 保持隔离环境 |

## 6. Conclusion

The dynamic analysis indicates that the chat system initializes an RSA-4096 key pair and attempts a local MongoDB connection, which fails due to no-network mode.  
No external connections, file tampering, or command execution were observed. The primary issue is weak error handling and potential misconfiguration risk.  
Overall risk rating: Moderate.  
  
动态分析结果表明，该聊天系统在启动阶段生成 RSA 密钥并尝试连接本地 MongoDB 数据库，在禁网环境下连接失败。  
未发现外部通信、文件植入或命令执行行为。主要问题为异常处理不足及数据库配置风险。总体安全评级：中等。