网络安全隐患报告

长沙市生态环境局：

政务网络安全运营中心监测发现，长沙市生态环境局所属重点污染源自动监控与基础数据库存在Swagger UI页面未授权访问。经验证，在未经身份验证的情况下，可直接访问接口文档，获取敏感接口信息，存在安全风险，请根据附件完成事件处置以及相关整改工作。

附件：1.事件详情及整改建议

城市网络安全运营中心

2024年7月29日

附件1

事件详情及整改建议

一般·中危

一、系统名称

重点污染源自动监控与基础数据库系统

二、隐患详情

1.隐患类型

Swagger UI页面未授权访问

2.危害描述

由于未对系统权限进行正确的配置，导致攻击者可以直接访问Swagger接口文档，任意查看敏感接口，存在较大安全隐患。

3.受影响面

URL:http://172.26.163.196:8888/v2/api-docs

4.隐患验证



图1 告警列表

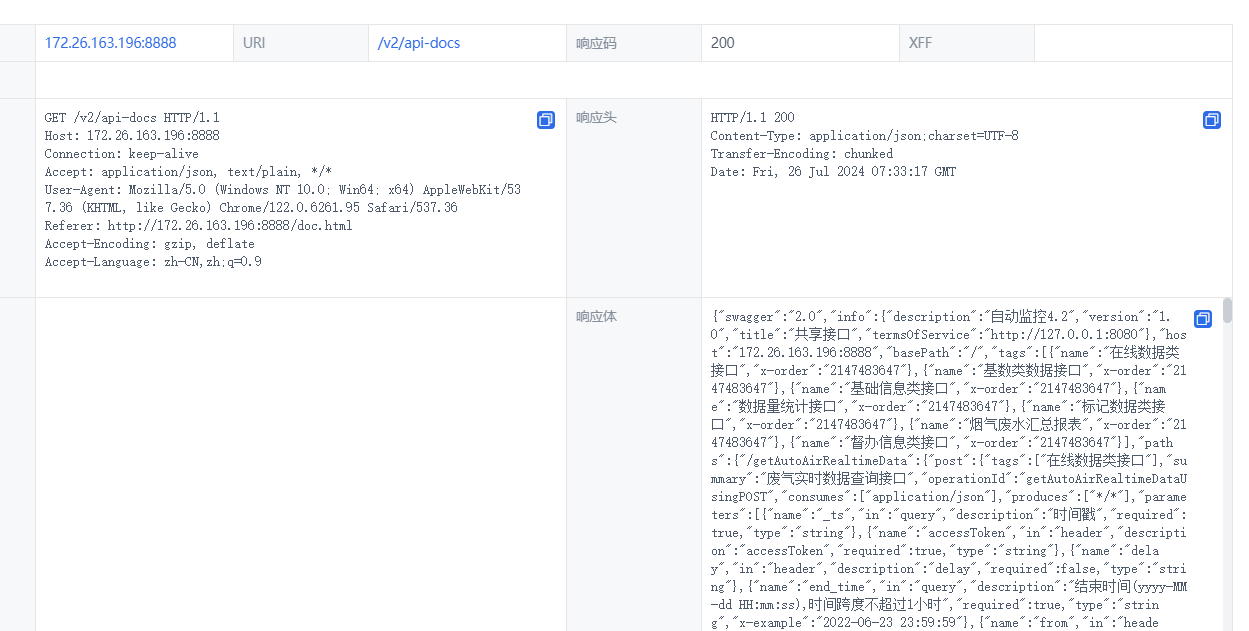


图2 告警详情

三、整改建议

1.在生产环境禁用Swagger；

2.禁用敏感接口，或针对开放接口启用鉴权认证和授权控制，可采用包含数字证书或公私钥对的方式进行双向身份认证；

3.在接口调用数据传输中，对传输数据进行加密，防止数据被窃听或泄露；

4.建立API安全网关，对于常规漏洞进行防护检测，比如SQL注入、XSS、RCE等。