**容器安全报告**

# **报告概览**

报告日期：2023年12月22日

报告版本：1.0

扫描对象：容器云平台

扫描范围：全部容器镜像及运行时环境

# **漏洞摘要**

严重漏洞：4个

高危漏洞：10个

中危漏洞：15个

低危漏洞：20个

# **重点漏洞详情及建议措施**

CVE-2023-0001: SQL注入  
 严重性：严重  
 影响组件：数据库服务  
 详细建议：更新至最新版本的数据库软件以修复已知漏洞。实施严格的输入验证措施。使用参数化查询和预处理语句。对数据库访问进行最小权限配置。  
 状态：待修复

CVE-2023-0025: 跨站脚本攻击 (XSS)  
 严重性：高  
 影响组件：Web应用界面  
 详细建议：对所有用户输入进行字符过滤和转义处理。实施内容安全策略（CSP）。使用安全工具进行代码审查。提高开发人员的安全编码意识。  
 状态：修复中

CVE-2023-0018: 容器逃逸  
 严重性：严重  
 影响组件：容器运行时  
 详细建议：更新容器管理工具和运行时环境。对容器进行资源限制和隔离。实施角色基于访问控制（RBAC）。定期检查和更新容器的安全配置。  
 状态：待修复