# XUGUCONSOLE-AP-2025-073010漏洞修复操作手册

## 1. 安全漏洞术语

| | |
|---|---|
| 漏洞类型 | SQL注入漏洞、权限管理漏洞、配置错误漏洞、数据泄露漏洞、缓冲区溢出漏洞、未授权访问漏洞、社会工程攻击、日志泄露漏洞、过度依赖第三方插件、未及时更新和修补、默认密码和设置、物理安全漏洞、备份和恢复漏洞、脚本注入漏洞、数据库审计不足、缺乏加密措施等 |
| CVE | 全球统一的漏洞编号标准，由MITRE维护，用于跨组织漏洞信息共享（如CVE-2024-1234） |
| CVSS | 通用漏洞评分系统，量化漏洞严重性 |
| 0Day漏洞 | 未被公开披露或无官方补丁的漏洞，攻击者可利用时间差发起攻击 |
| CNNVD | 中国国家信息安全漏洞库，是由中国信息安全测评中心建设运维的国家级漏洞库，收录漏洞并分配CNNVD编号 |
| CNVD | 国家信息安全漏洞共享平台，中国国家级漏洞库，收录漏洞并分配CNVD编号 |
| NVDB | 网络安全威胁和漏洞信息共享平台，是由工业和信息化部网络安全管理局组织建设的国家级平台，收录漏洞并分配NVDB编号 |

## 2. 漏洞基本属性

### 2.1 漏洞信息

| | |
|---|---|
| 漏洞编号 | 内部编号：XUGUCONSOLE-AP-2025-073010<br>外部编号：CNNVD-2024-96348367 |
| 漏洞名称 | XuguConSole 内存越界漏洞 |
| 漏洞类型 | 二进制类 |
| 发现时间 | 2025年7月30日 |
| 发现渠道 | CNNVD平台安全漏洞 |
| 影响版本 | XuguConsole版本 ＜ XuguConsole V2 |

| | |
|---|---|
| CVSS评分 | 2.2 |
| 修复时间 | 2025-01-01 |
| 修复版本 | XuguConsole V2 |

## 2.2 漏洞描述

| | |
|---|---|
| 技术原理 | `漏洞位置与成因`：xgconsole在使用SPOOL函数导出数据时，未对用户提供的导出路径进行有效校验与过滤，允许将路径设置为根目录“/”<br>`攻击手法`：当该路径参数被传递至 `fopen()` 函数进行解析，并后续由 `fprintf()` 函数以 `%s` 格式符处理时，由于路径字符串异常，引发了内存越界访问。 |
| 攻击向量 | 攻击者通过可控的输入渠道向使用该漏洞函数的程序提供恶意构造的字符串，造成内存越界访问攻击 |
| 潜在危害 | 通过内存越界访问攻击，fopen解析后，fprintf使用%s时对应的参数内存越界，产生崩溃。 |

# 3. 漏洞规避方案

此漏洞为控制台漏洞，仅对客户端产生影响，且需要用户对所输入内容进行精心构造，因此实际危害性较低，仅需用户避免使用相关风险语句场景。

# 4. 漏洞修复方案

用户可通过版本补丁升级的方式进行漏洞的修复，即下载修复后的虚谷控制台版本，进行版本迭代，以规避上述漏洞内容。

## 4.1 官方漏洞补丁下载

从 XuguDB 官方网站（官方网址：www.xugudb.com）查询并获取安全漏洞公告，随后依据公告指引，下载对应目标平台（Windows X86_64、Linux X86_64、Linux Aarch64）的安全漏洞补丁文件。

**补丁下载地址**：https://download.xugudb.com/XuguDB-Console-2.2.2-linux-x86_64-20250714.zip

## 4.2 修复前的准备工作

（1）数据备份：条件具备情况下，对生产环境 XuguDB 实例进行完整备份，覆盖所有数据文件和日志文件。

（2）实验验证：复制数据库生产环境配置（包括XuguDB版本、操作系统），使用虚拟机或容器技术隔离测试环境，在隔离测试环境按照下述漏洞修复步骤进行测试验证，确认漏洞已完全修复，并演练修复过程。

## 4.3 安全漏洞正式修复

### 步骤一：上传漏洞补丁文件(具体以实际安装路径为准)，并更换控制台二进制进程文件

代码块

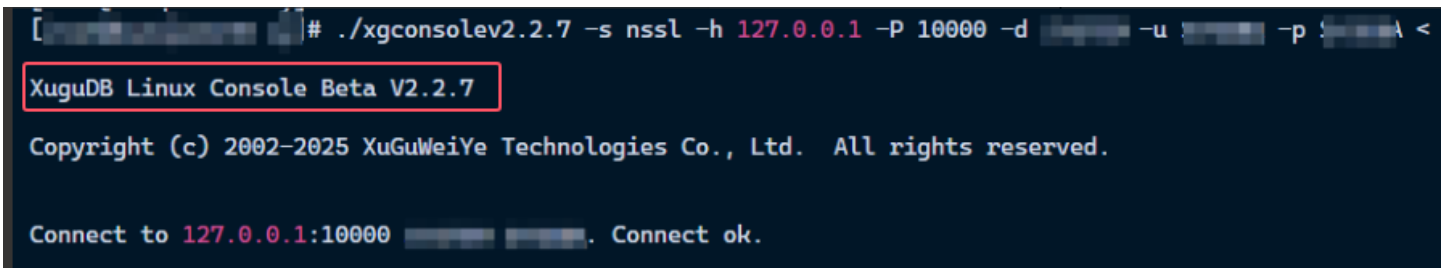
```
-- 进入数据库安装目录下的BIN目录
[root@localhost XuguDB]# cd /opt/xugu/Client/xgconsole

-- 解压补丁包，补丁文件（如：xgconsole）
-- 替换 xgconsole目录下原有的二进制进程文件（或直接使用新的补丁文件）

-- 备份原有的历史程序文件
[root@localhost XuguDB]# mv xgconsole_历史程序文件  xgconsole_历史程序文件.bak
-- 替换原有控制台文件，以实际文件名为准
[root@localhost XuguDB]# mv xgconsole_v2 xgconsole_v1
```

# 5. 修复版本验证

在连接数据库的过程中，相关控制台界面会自动输出所对应版本




根据XuguConsole控制台所显示的版本，确认当前版本满足安全漏洞修复要求的最低修复版本要求。

# 6. 后续注意事项

**记录留存**：将漏洞修复过程（如操作时间、执行人员、使用的补丁版本、验证结果）记录到《漏洞修复记录表》（附表格模板），便于后续追溯。

**定期检查**：建议每月执行一次漏洞扫描，及时发现新漏洞（如需支持，可联系我司技术支持人员）。

**安全加固**：除漏洞修复外，可通过以下措施提升系统安全性：

- 提升登录用户密码强度，并定期更换登录用户密码（建议：每 1 个月一次）；

- 最小化原则配置管理权限；

- 及时关注官方安全漏洞公告，及时修复已知漏洞。

## 7. 技术服务支持

若在漏洞修复过程中遇到问题，可通过以下方式联系官方技术支持：

服务热线：400-888-6236（工作时间：周一至周五 9:00-18:00）

技术邮箱：technology@xugudb.com（请注明 “漏洞修复求助”，并附上异常截图与操作记录）

在线客服：官网 “在线咨询” 板块实时咨询（http://www.xugudb.com）

# 附件：漏洞修复记录表

| 漏洞编号 | 漏洞名称 | 补丁版本 | 修复时间 | 修复状态 | 执行人员 |
| --- | --- | --- | --- | --- | --- |
| | | | | | |