

XUGUCM-AP-2025-073007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：XUGUCM-AP-2025-073007 外部编号：CNNVD-2024-51578181
漏洞名称	XuguCM 信息接口存在xss漏洞
漏洞类型	XSS漏洞
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	XuguCM版本 ≤ XuguCM-2.13.0
CVSS评分	2.0

修复时间	2025-07-24
修复版本	XuguCM-2.13.1

2.2 漏洞描述

技术原理	漏洞位置与成因：未对alterNode接口中用户输入的相关参数进行严格校验 攻击手法：通过精心构造相关语句内容，可实现反射性XSS漏洞
攻击向量	登录系统后台后，通过此漏洞进行xss攻击，获取相关用户信息
潜在危害	通过此漏洞，攻击者可攻击此系统，可获取系统内用户的相关认证信息，例如cookie等信息

3. 漏洞规避方案

该漏洞主要因为未对用户输入内容进行严格校验，导致攻击者可通过此漏洞运行恶意的JS脚本。虚谷数据库集群监控软件补丁通过对用户输入内容进行严格校验处理该漏洞。

此漏洞为后台漏洞。需登录后台执行，漏洞规避建议如下：

代码块

- 1 修改系统密码为强密码，要求设置不少于八位的密码。且包含大小写字母，特殊符号以及数字的组合，定期修改密码

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监控平台版本，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/XuguCM-2.13.1.20250724-beta02-linux-x64.tar.gz>

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，解压程序包 XuguCM-*.tar.gz 到任意目录。

代码块

```
1  -- 备份原有的历史程序文件
2  [root@localhost XuguDB]# mv XuguCM_历史程序文件 XuguCM_历史程序文件.bak
3
4  -- 进入你希望解压软件包的目录，(需放置新的路径)。
5  [root@localhost XuguDB]# cd /path/to/your/target_directory
6
7  -- 解压补丁包，补丁文件（如：XuguCM-*.tar.gz）
8  [root@localhost XuguDB]# tar -xzf XuguCM-*.tar.gz
```

步骤二：进入程序目录，执行 startdb.sh，启动数据库

代码块

```
1  [root@localhost XuguDB]# ./startdb.sh
```

步骤三：修改bin/catalina.sh JAVA_OPTS参数

代码块

```
1  修改bin/catalina.sh的--JAVA_OPTS参数 -
   DallowedHosts=127.0.0.1:8080,192.168.2.215:8080，将默认的127.0.0.1:8080(本地访问，
   只需修改端口)和192.168.2.215:8080修改为监控所在服务器的ip和端口(远程访问，ip和端口都需要修改)
2  [root@localhost XuguDB]# vim bin/catalina.sh
```

步骤四：进入程序目录，执行 startapp.sh，启动监控服务。

代码块

```
1  [root@localhost XuguDB]# ./startapp.sh
```

步骤四：访问相关站点

- 1 --使用浏览器访问所设置的IP以及端口，观察服务是否正常运行
- 2 例如访问<http://127.0.0.1:8080/xgcm/login>

5. 修复版本验证

登录进入系统后，观察系统内部所显示的版本与修复版本是否相对应

根据XuguCM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. 技术支持支持

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