

XUGUDB-AP-2025-052704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：XUGUDB-AP-2025-052704 外部编号：CNNVD-2025-73585748
漏洞名称	XuguDB普通用户越权漏洞
漏洞类型	权限管理类
发现时间	2025年6月3日
发现渠道	CNNVD平台安全漏洞
影响版本	XuguDB V11.0 版本 ≤ XuguDB V11.0 BuildTime 2025-04-07 11:00:00 r13 by XuGu
CVSS评分	9.1

修复时间	2025年6月16日
修复版本	XuguDB V11.0 BuildTime 2025-06-12 11:00:00 r14 by XuGu

2.2 漏洞描述

技术原理	DBA_USERS 系统视图：仅允许管理员访问，包含完整用户信息 ALL_USERS 系统视图：普通用户可访问，仅显示权限范围内可见的账户信息 普通用户通过 ALL_USERS 视图获取了所有用户的密码哈希值，突破了最小权限原则，导致敏感信息泄露风险
攻击向量	横向渗透或密码爆破：普通登录用户使用工具对特定用户密码哈希值进行暴力破解或字典攻击，若用户密码复杂度低，破解率显著提升
潜在危害	非授权用户的PASSWORD加密密文数据可见性查看，越权查看

3. 漏洞规避方案

该漏洞主要因为普通用户可访问all_users表，查询到有权限查看的其他用户信息，包含了密码等字段内容。虚谷数据库补丁通过限制用户可见性处理该漏洞。

若暂无法通过版本补丁升级的方式进行处理，规避方案如下：

强化密码策略，加强用户密码的复杂度，增加破解难度，并设置连续多次密码验证错误登录IP临时锁定。

代码块

```
1  -- 口令的最短长度为8
2  SQL> SET MIN_PASS_LEN TO 8;
3
4  -- 口令模式 1:不重复字符或数字,2:字母+数字,3:字母+数字+符号
5  SQL> SET PASS_MODE TO 3;
6
7  -- 三次登录失败，锁定登录失败 IP 地址
8  SQL> SET CONN_FAIL_CNT TO 3;
```

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数据库版本，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/security-patches/XUGUDB/v11/linux-x64/XUGUDB-V11D20250616-SP004.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：停止业务应用，确定数据库负载已停止

- (1) 由业务系统运维人员停止业务系统服务或中间件
- (2) 查询XuguDB数据库连接是否完全断开，数据库负载是否已终止

代码块

```
1  -- 使用管理员账号登录数据库服务器
2  [root@localhost console]#./xgconsole -s nssl -h 数据库IP地址 -P 数据库访问端口 -d
   系统数据库 -u 超级管理员 -p 用户密码
3  Server [127.0.0.1]:
4  Port [51381]:
5  SSL [nssl]:
6  Database [SYSTEM]:SYSTEM
7  Username [SYSDBAT: SYSDBA
8  please input password:*masked*
9  XuguDB Linux Console GA V2.2.2
10 Copyright(c)2002-2025 XuGuWeiYe Technologies co.,Ltd. All rights reserved.
11 Connect to 127.0.0.1:5138 SYSTEM SYSDBA. Connect ok.
12
13 -- XuguDB查询系统内是否有活跃会话
14 SQL>SELECT USERNAME, DB_NAME, IP, STATUS,curr_tid FROM SYS_ALL_SESSIONS WHERE
   STATUS <> 114;
15
16 -- 若有活跃会话则业务层进行终止
17 -- 若业务层评估可以数据库内部进行事务kill，执行下面的命令
18 -- 第一个参数为事务所在的数据节点号，第二个参数为上述会话表查询的curr_tid
19 SQL>exec DBMS_DBA.KILL_TRANS(节点号, 事务号);
```

步骤二：SHUTDOWN数据库服务，并确认服务停止

代码块

```
1  -- 确认无活跃会话则业务层进行终止后，执行下面的关机命令
2  SQL>shutdown immediate;
3
4  -- 确认数据库服务终止，进程停止（无对应数据库进程）
5  [root@localhost XuguDB]# ps -ef|grep xugu
6
7  -- 进行数据库冷备份（可选）
8  [root@localhost XuguDB]# cp -r HOME BAK_HOME
```

步骤三：上传漏洞补丁文件(具体以实际安装路径为准)，并更换数据库二进制进程文件

代码块

```
1  -- 进入数据库安装目录下的BIN目录
2  [root@localhost XuguDB]# cd /opt/xugu/db/BIN
3
4  -- 解压补丁包，补丁文件（如：xugu_linux_x86_64_20250327）
5  -- 替换 BIN 目录下原有的二进制进程文件（或直接使用新的补丁文件）
6
7  -- 备份原有的历史程序文件
8  [root@localhost XuguDB]# mv xugu_linux_x86_64_历史程序文件 xugu_linux_x86_64_历史程序文件.bak
9  -- 更名补丁程序为正式文件名
10 [root@localhost XuguDB]# mv xugu_linux_x86_64_20250327 xugu_linux_x86_64
11
```

步骤四：启动XuguDB数据库服务，并检查数据库状态状态

代码块

```
1  -- 进入数据库安装目录下的BIN目录（执行命令：cd /opt/xugu/db/BIN，路径以实际为准）
2  [root@localhost XuguDB]# $/PWD/xugu_linux_x86_64 -service
3
4  -- 在 BIN 目录下输入命令，查看数据库启动日志
5  [root@localhost XuguDB]# tail -f stdout.txt
6  -- 当日志中出现 “Listening at port 5138”（端口号以客户实际配置为准），说明数据库启动成功。
```

步骤五：检查数据库服务状态

代码块

```
1  -- 使用管理员账号登录数据库服务器
2  [root@localhost console]#./xgconsole -s nssl -h 数据库IP地址 -P 数据库访问端口 -d
    系统数据库 -u 超级管理员 -p 用户密码
3  Server [127.0.0.1]:
4  Port [51381]:
5  SSL [nssl]:
6  Database [SYSTEM]:SYSTEM
7  Username [SYSDBAT: SYSDBA
8  please input password:*masked*
9  XuguDB Linux Console GA V2.2.2
10 Copyright(c)2002-2025 XuGuWeiYe Technologies co.,Ltd. All rights reserved.
11 Connect to 127.0.0.1:5138 SYSTEM SYSDBA. Connect ok.
12
13 SQL>
14 -- 查看数据库服务节点状态
15 SQL>SHOW CLUSTERS
```

5. 修复版本验证

代码块

```
1  -- 查询当前XuguDB数据库版本
2  SQL>show version
3
4  -- 查询当前XuguDB数据库编译时间
5  SQL>show build_time
```

根据XuguDB查询所获得的版本及编译时间信息，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