XUGUDB-AP-2025-101002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-2025-101002 外部编号：CNNVD-2025-42002507
漏洞名称	虚谷数据库 ROUND函数存在拒绝服务漏洞
漏洞类型	二进制类
发现时间	2025年10月10日
发现渠道	CNNVD平台安全漏洞
影响版本	XuguDB V12.0 版本 < XuguDB V12.10.1
CVSS评分	5.7

修复时间	2024-09-26
修复版本	XuguDB V12.10.1

2.2 漏洞描述

技术原理	ROUND函数内部实现中，未对用户传入的“保留小数位数”参数进行有效的范围校验与限制，允许其超出函数设计预期或底层计算单元的安全边界。该参数传入极大或极小的异常值时，触发内部大数运算发生缓冲区或数值越界， 可导致进程崩溃、数据计算错误。
攻击向量	攻击者通过可控的输入渠道传入异常小数位参数触发越界
潜在危害	内存越界致服务崩溃

3. 漏洞规避方案

该漏洞主要因为未对用户输入的内容进行校验，以及代码层面校验不充分。虚谷数据库补丁通过修改相关函数理该漏洞。

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：

相关漏洞需要用户登录。因此通过强化密码策略，加强用户密码的复杂度，防止外部非可信人员登录数据库进行规避。

代码块

```
-- 口令的最短长度为8
SQL> SET MIN_PASS_LEN TO 8;

-- 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
SOL> SET PASS_MODE TO 3;

-- 三次登录失败，锁定登录失败 IP 地址
SOL>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：http://download.xugudb.com/security-patches/XUGUDB/v12/linux-x64/XuguDB-Server-12.10.1-linux-x86_64-20250926-Beta.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

```
-- 使用管理员账号登录数据库服务器
[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
Server [127.0.0.1l:
Port [51381]:
SSL [nssl]:
Database [SYSTEM]:SYSTEM
Username [SYSDBAT: SYSDBA
please input password:*masked*
XuguDB Linux Console GA V2.2.2
Copyright(c)2002-2025 XuGuWeiYe Technologies co.,Ltd. All rights reserved.
Connect to 127.0.0.1:5138 SYSTEM SYSDBA. Connect ok.

-- XuguDB查询系统内是否有活跃会话
SQL>SELECT USERNAME, DB_NAME, IP, STATUS,curr_tid FROM SYS_ALL_SESSIONS WHERE STATUS  <> 114;

-- 若有活跃会话则业务层进行终止
-- 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
-- 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
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

```
-- 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
SQL>shutdown immediate;

-- 确认数据库服务终止，进程停止（无对应数据库进程）
[root@localhost XuguDB]# ps -ef|grep xugu

-- 进行数据库冷备份（可选）
[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

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

-- 解压补丁包，补丁文件（如：xugu_linux_x86_64_20250327）
-- 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）

-- 备份原有的历史程序文件
[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
-- 更名补丁程序为正式文件名
[root@localhost XuguDB]# mv xugu_linux_x86_64_20250327 xugu_linux_x86_64

```

步骤四：启动XuguDB数据库服务，并检查数据库状态状态

代码块

```
-- 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）
[root@localhost XuguDB]# $/PWD/xugu_linux_x86_64 -service

-- 在 BIN 目录下输入命令，查看数据库启动日志
[root@localhost XuguDB]# tail -f stdout.txt
-- 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

```
-- 使用管理员账号登录数据库服务器
```

```
[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
Server [127.0.0.1l:
Port [51381]:
SSL [nssl]:
Database [SYSTEM]:SYSTEM
Username [SYSDBAT: SYSDBA
please input password:*masked*
XuguDB Linux Console GA V2.2.2
Copyright(c)2002-2025 XuGuWeiYe Technologies co.,Ltd. All rights reserved.
Connect to 127.0.0.1:5138 SYSTEM SYSDBA. Connect ok.

SQL>
-- 查看数据库服务节点状态
SQL>SHOW CLUSTERS
```

5. 修复版本验证

代码块

```
-- 查询当前XuguDB数据库版本
SQL>show version

-- 查询当前XuguDB数据库编译时间
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