

# XuguDB

## DBMS\_REPLICATION.CREATE\_ MODIFY\_SOURCE 函数栈溢出漏洞

### 修复操作指导手册

#### 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（如 CVSS 3.1 评分 $\geq$ 9.0 为超危）
热修复	漏洞热修复（Hot Fix）是指在不中断系统运行或无需重启服务的情况下，通过动态加载补丁或更新程序来实时修复软件漏洞的技术方案。
冷修复	漏洞冷修复（Cold Fix）是指需要停止系统或服务运行，通过重启或重新部署补丁文件来完成漏洞修复的技术方案。
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
SQL 注入	通过恶意 SQL 语句操控数据库（如 ' OR 1=1 --绕过认证）

## 2. 漏洞基本属性

### 2.1 漏洞信息

漏洞编号	CNNVD-2024-72259516
漏洞名称	DBMS_REPLICATION.CREATE_MODIFY_SOURCE 函数栈溢出漏洞
漏洞类型	栈溢出漏洞
发现时间	2025 年5月27日
发现渠道	CNNVD 通报
影响版本	XuguDB 11.0.0 Build_time:2025-06-12 11:00:00 r14 by XuGu 之前版本
CVSS 评分	9.8
修复时间	2025-06-16
修复版本	XuguDB 11.0.0 Build_time:2025-06-12 11:00:00 r14 by XuGu

### 2.2 漏洞描述

技术原理	虚谷数据库服务端程序 DBMS_REPLICATION.CREATE_MODIFY_SOURCE 函数中存在栈溢出漏洞，可导致远程代码执行。。
攻击向量	栈溢出漏洞
潜在危害	二进制漏洞

### 3. 漏洞规避方案

限制相关 IP 访问，设置连接白名单

典型场景防护规避方案：

漏洞类型	漏洞描述	临时规避手段	适用场景
SQL 注入	攻击者通过输入恶意 SQL 代码操控数据库	<ol style="list-style-type: none"><li>启用输入过滤（拦截 '、;、DROP 等字符）</li><li>强制使用参数化查询（预编译语句）</li><li>临时启用数据库防火墙拦截恶意语句</li></ol>	登录表单、搜索功能等用户输入场景
弱密码/默认密码	使用简单密码或未修改默认账户密码	<ol style="list-style-type: none"><li>强制密码复杂度策略（pass_mode=3，含大小写字母+符号）</li><li>临时禁用默认账户并重置密码</li></ol>	管理员账户、服务账户等敏感权限账户
未授权访问	未配置权限控制导致攻击者直接访问敏感数据	<ol style="list-style-type: none"><li>临时启用 IP 白名单限制访问来源</li><li>部署基于角色的访问控制（RBAC）</li><li>关闭非必要服务端口</li></ol>	开发测试环境、内部系统接口
数据泄露	敏感数据明文存储或传输被截获	<ol style="list-style-type: none"><li>临时启用 SSL/TLS 加密传输</li><li>对敏感字段进行哈希加密（如 SHA-256）</li><li>限制备份文件访问权限</li></ol>	数据库配置、备份文件、网络传输场景
DDoS 攻击	大量恶意请求导致数据库服务不	<ol style="list-style-type: none"><li>配置流量清洗设备或云服务商 DDoS 防护</li><li>启用连接数限制（如数据</li></ol>	高并发业务场景、公网暴露的数据库

	可用	库连接池、OS socket) 3. 切换至灾备节点	服务
默认配置漏洞	使用默认端口、未禁用危险功能 (如远程管理)	1. 修改默认端口 (如 5138 改为随机端口) 2. 临时关闭远程管理功能	新部署数据库、遗留系统
缓冲区溢出	输入数据超出缓冲区限制触发代码执行	1. 限制输入长度 (如用户名 ≤50 字符) 2. 启用安全编码规范 3. 临时部署入侵检测系统 (IDS) 监控异常请求	C/S 架构应用、自定义协议交互场景
备份数据泄露	备份文件未加密或存储位置不安全	1. 临时加密备份文件 (如使用 AES-256) 2. 将备份存储至离线介质或私有云 3. 设置备份文件访问审计日志	定期备份流程、灾难恢复演练
权限滥用	高权限账户被内部人员滥用	1. 临时启用操作日志记录 (记录 GRANT、DELETE 等行为) 2. 实施双人复核机制 (关键操作需两人授权) 3. 收回非必要的高权限账户	财务系统、核心业务数据库
会话劫持	攻击者窃取 Session ID 后冒充合法用户	1. 缩短会话有效期 (如 30 分钟自动过期) 2. 启用 HttpOnly 和 Secure 标志的 Cookie 3. 强制定期重新认证	用户登录态保持、跨域服务调用
供应链攻击	第三方组件存在未修复漏洞	1. 临时禁用高风险组件 2. 限制组件访问 IP 范围 3. 部署网络隔离 (如 VLAN 划分)	使用开源中间件的系统、微服务架构

## 4. 漏洞修复方案

### 4.1 修复前准备工作

准备项	具体要求
数据备份	<ol style="list-style-type: none"><li>1. 备份受影响系统的关键数据（如数据库文件、配置文件、业务数据等）；</li><li>2. 确认备份文件可正常恢复（建议先测试恢复流程）。</li></ol>
操作环境	<ol style="list-style-type: none"><li>1. 确保操作设备（如运维电脑）与受影响设备网络连通，且具备操作权限；</li><li>2. 关闭无关应用。</li></ol>
修复工具 / 补丁	<ol style="list-style-type: none"><li>1. 从虚谷官方渠道获取漏洞修复所需的补丁包、升级程序或配置工具（附官方下载地址）；</li><li>2. 验证补丁完整性（如核对 MD5 值，避免使用第三方非官方文件）。</li></ol>

### 4.2 漏洞修复步骤

#### 4.2.1 漏洞修复通用流程

步骤	操作内容	操作详情
1	获取补丁文件	<ol style="list-style-type: none"><li>1. 从虚谷官方渠道获取对应漏洞修复所需的补丁文件</li><li>2. 将补丁文件下载到本地。</li></ol>
2	仿真环境启动	<ol style="list-style-type: none"><li>1. 仿真环境中启动修复后的补丁文件</li><li>2. 启动应用测试是否异常</li></ol>
3	业务切割时间与数据备份方案	<ol style="list-style-type: none"><li>1. 沟通业务停机窗口期</li><li>2. 查询业务数据量，沟通采用不停机热备份或者停机冷备份</li></ol>

4	登录虚谷数据库服务器并进入 SQL 命令行界面	1. 使用管理员账号登录数据库服务器；2. 打开 SQL 命令行界面，输入账号密码完成登录（确保登录账号具备数据库停机权限）。
5	业务停机与热备份	<ol style="list-style-type: none"> <li>1. 业务运维人员停止业务系统</li> <li>2. 虚谷技术支持人员查询数据库连接是否完全断开，查询业务是否完全停止</li> <li>3. 执行 <code>backup database</code> 命令进行数据热备份操作</li> </ol>
6	停机操作与冷备份	<ol style="list-style-type: none"> <li>1. 在 SQL 命令行界面输入命令：<code>shutdown</code>；执行数据库停机</li> <li>2. 执行 <code>ps -ef grep xugu</code> 命令检查数据库停机状态</li> <li>3. 进入所有的数据库目录，执行 <code>cp -r HOME BAK_HOME</code> 进行数据库文件冷备份</li> </ol>
7	上传补丁文件并替换启动文件	<ol style="list-style-type: none"> <li>1. 将本地下载的补丁文件上传到虚谷数据库的“BIN 目录”（如：<code>/opt/xugu/db/BIN</code>，具体以客户实际安装路径为准）；</li> <li>2. 解压补丁文件，将补丁中的启动文件（如：<code>xugu_linux_x86_64_20250327</code>）替换 BIN 目录下原有的启动文件。</li> </ol>
8	重启虚谷数据库	1. 在服务器命令行界面进入 BIN 目录（执行命令： <code>cd /opt/xugu/db/BIN</code> ，路径以实际为准）；2. 输入启动命令： <code>\$/PWD/xugu_linux_x86_64_20250327 - service</code> ，按下回车启动数据库。
9	检查数据库重启状态	1. 在 BIN 目录下输入命令： <code>tail -f stdout.txt</code> ，查看数据库启动日志；2. 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，可按“Ctrl+C”退出日志。
10	启动业务应用	业务运维人员启动业务应用，观察业务运行是否正常

## 5. 修复验证测试

## 5.1 版本验证（针对补丁升级类漏洞）

Plain Text

```
-- 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，确认当前版本是否为本文档安全漏洞修复要求的最低修复版本。

## 5.2 漏洞复测（专项验证）

**操作依据：**参照漏洞原发现报告（或我方提供的《漏洞验证方案》）中记录的漏洞触发条件、测试步骤及工具，在修复后的虚谷数据库环境中复现测试操作。

**测试内容：**参照漏洞原触发步骤在修复后环境中执行验证操作，确认漏洞现象已消除且无复现情况。

**判定标准：**测试过程中未出现漏洞原有的异常现象，且连续 3 次复测结果一致，判定漏洞已修复，无复现风险。

**功能验证：**检查受影响系统 / 设备的核心功能是否正常（如业务系统能否正常登录、数据能否正常读写、网络设备能否正常转发数据）。

### 5.2.1 异常处理

常见异常	解决方案
修复后系统无法启动	1. 重启设备，尝试进入安全模式（Windows 按 F8，Linux 按 Grub 菜单选择）；2. 若安全模式可进入，卸载已安装的补丁，恢复到修复前状态；3. 联系我方技术支持，提供异常截图与操作记录。
业务功能异常（如无法访问）	1. 检查修复过程中是否修改了关键配置（如端口、IP 地址），若有则恢复原配置；2. 恢复数据备份（使用修复前备份的文件），重新测试功能。
漏洞仍显示“未修复”	1. 确认补丁安装是否成功（查看安装日志，是否有“安装失败”提示）；2. 从官方渠道重新下载补丁，再次执行修复操作；3.

确认漏洞是否存在多个修复点，是否遗漏操作。

## 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（可使用我方提供的漏洞扫描服务，如有需求可联系支持人员）。

安全加固：除漏洞修复外，可通过以下措施提升系统安全性： - 定期更换管理员密码（每 3 个月一次）； - 关闭不使用的服务与端口； - 安装杀毒软件并开启实时防护。

## 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](mailto: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	修复时间	修复状态	执行人员
CNNVD-2025-73585748	虚谷数据库普通用户越权漏洞	2025-06-16 09:00	已修复	聂勋
CNNVD-2024-08898016	虚谷数据库权限管理缺陷漏洞	2025-06-16 09:00	已修复	聂勋
CNNVD-2024-72259516	DBMS_REPLICATION.CREATE_MODIFY_SOURCE 函数栈溢出漏洞	2025-06-16 09:00	已修复	聂勋