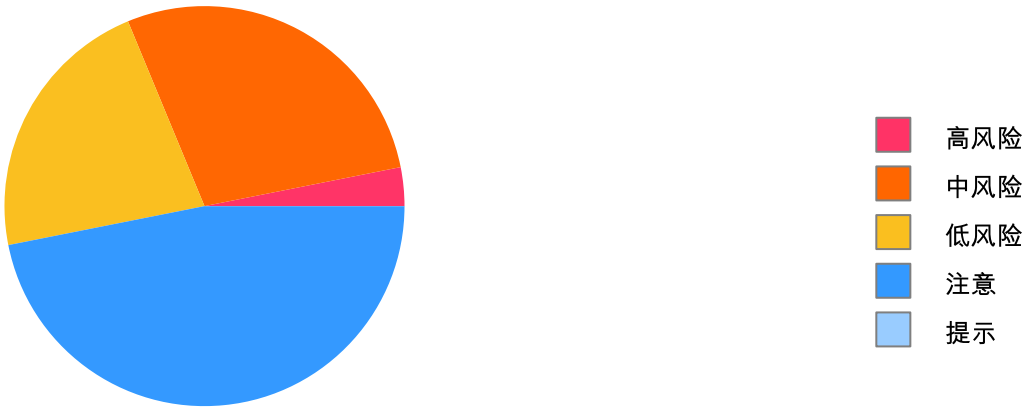
重点污染源自动监控系统与基础数据库系统V4.2(国发平台)
数据库安全评估报告

1 综述信息

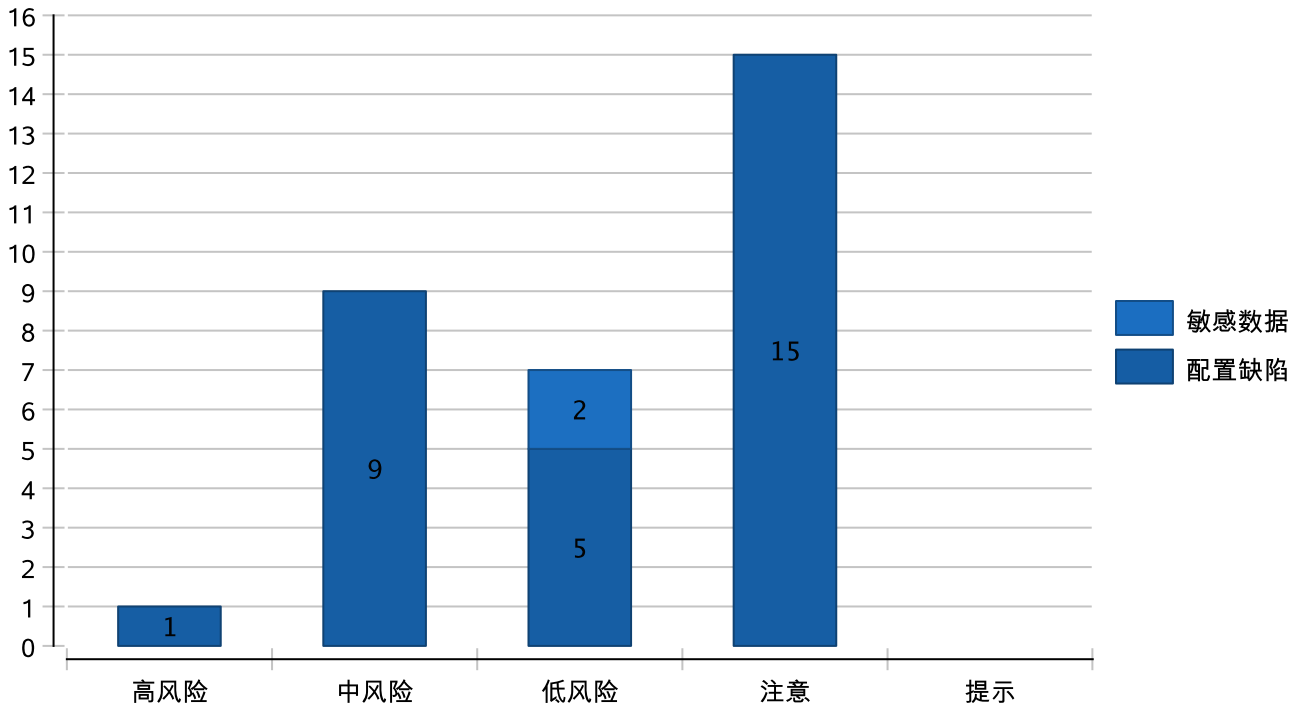
1.1 任务信息

任务名称	综合检测任务20231114_3_漏洞扫描任务20231114_34	IP地址	10.202.6.125
策略	全面扫描	端口号	5432
扫描用时（秒）	2	数据库类型	PostgreSQL
开始时间	2023-11-14 16:09:16	数据库版本号	
结束时间	2023-11-14 16:09:18	实例名	amdb

1.2 风险分布-风险等级



1.3 风险分布-风险类别



2 检测结果

ip地址	高风险	中风险	低风险	注意	提示	总计
10.202.6.125	1	9	7	15	0	32

2.1 弱口令信息

用户名	密码	用户状态	弱口令类型	风险等级

2.2 漏洞检测结果

风险等级	检测项类型	检测项名称	CVE
高风险	配置缺陷	检查是否回收public模式的所有权限	
中风险	配置缺陷	确保log_checkpoints选项开启	
中风险	配置缺陷	确保log_disconnections选项开启	
中风险	配置缺陷	确保log_statement设置为ddl	
中风险	配置缺陷	确保log_timezone设置为gmt	
中风险	配置缺陷	确保log_temp_files设置为0	
中风险	配置缺陷	确保log_duration选项开启	
中风险	配置缺陷	确保log_connections选项开启	
中风险	配置缺陷	确保logging collector开启	
中风险	配置缺陷	确保SSL正确配置	
低风险	配置缺陷	使用了缺省连接端口5432	
低风险	配置缺陷	检查示例数据库是否删除	
低风险	配置缺陷	ALTER USER/CREATE USER设置默认用户密码时没有启用加密	
低风险	配置缺陷	配置了非缺省的 Unix socket 权限	
低风险	敏感数据	从PostgreSQL的INFORMATION_SCHEMA.COl表获取到可能包含密码信息的列	
低风险	敏感数据	获取到包含密码的函数和存储过程(Postgresql)	
低风险	配置缺陷	确保log_error_verbosity设置正确	
注意	配置缺陷	确保安装了set_user拓展应用	
注意	配置缺陷	确保Postmaster运行时参数配置正确	
注意	配置缺陷	确保Superuser运行时参数配置正确	

风险等级	检测项类型	检测项名称	CVE
注意	配置缺陷	确保PostgreSQL配置文件独立于数据簇之外	
注意	配置缺陷	检查超级用户权限授予情况	
注意	配置缺陷	检查登录权限授予情况	
注意	配置缺陷	检查create db权限授予情况	
注意	配置缺陷	确保User运行时参数配置正确	
注意	配置缺陷	确保'backend'运行参数设置正确	
注意	配置缺陷	确保PostgreSQL子目录位置在数据簇之外	
注意	配置缺陷	确保为流复制创建了专用用户	
注意	配置缺陷	检查密码有效期设置为永不过期的角色	
注意	配置缺陷	检查create role权限授予情况	
注意	配置缺陷	确保DML权限授予合理	
注意	配置缺陷	确保SIGHUP运行时参数配置正确	

2.2.1 高风险 检查是否回收public模式的所有权限

返回漏洞检测结果

检测项ID：	DBSEC_20190109_10
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查public权限的schema。默认情况下，PostgresSQL使用public schema，用于存储有关数据库，表，过程的信息。此schema可供所有用户访问，用户都可以查看每个表结构或过程，存在安全隐患。
修复建议：	建议回收public模式的所有权限。

2.2.2 中风险 确保log_checkpoints选项开启

返回漏洞检测结果

检测项ID：	DBSEC_20181125_15
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保log_checkpoints选项开启。启用检查点记录是跟踪频率的最简单方法和检查点操作的持续时间。
修复建议：	建议log_checkpoints选项开启:alter system set log_checkpoints = 'on';

2.2.3 中风险 确保log_disconnections选项开启

返回漏洞检测结果

检测项ID：	DBSEC_20181125_17
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保log_disconnections选项开启。启用log_disconnections设置将记录每个会话的结束时间，包括会话持续时间。此参数在会话启动后不能更改。PostgreSQL并不在内部维护连接的开始或结束，以供以后查看。只有启用这些日志记录功能，才能检查失败尝试的连接、“长时间”连接或其他异常情况。
修复建议：	建议log_disconnections选项开启:alter system set log_disconnections = 'on';

2.2.4 中风险 确保log_statement设置为ddl	返回漏洞检测结果
检测项ID：	DBSEC_20181125_21
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保log_statement设置为ddl。设置log_statement以与组织的安全性和日志记录策略保持一致 便于以后审核和审查数据库活动。
修复建议：	建议log_statement设置为ddl:alter system set log_statement='ddl';

2.2.5 中风险 确保log_timezone设置为gmt	返回漏洞检测结果
检测项ID：	DBSEC_20181125_24
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保log_timezone设置为gmt。log_timezone设置指定日志消息中时间戳中使用的时区。应根据您的定义为适当的时区配置日志条目时间戳 组织的日志记录策略，以确保在记录事件时不会产生混淆 发生了。
修复建议：	建议log_timezone设置为gmt:alter system set log_timezone = 'GMT';

2.2.6 中风险 确保log_temp_files设置为0	返回漏洞检测结果
检测项ID：	DBSEC_20181125_22
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保log_temp_files设置为0。将log_temp_files设置为0会导致记录所有临时文件信息 正值仅记录大小大于或等于指定数量的文件。如果未记录所有临时文件，则可能更难识别潜在的文件 可能是应用程序编码不佳或故意资源的性能问题 饥饿的尝试。
修复建议：	建议log_temp_files设置为0:alter system set log_temp_files = 0;

2.2.7 中风险 确保log_duration选项开启	返回漏洞检测结果
检测项ID：	DBSEC_20181125_18
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保log_duration选项开启。启用log_duration设置将记录每个完成的SQL语句的持续时间。对于使用扩展查询协议的客户端，解析、绑定和执行步骤的持续时间是独立记录的。通过记录语句的持续时间，很容易识别非性能查询和可能的DoS尝试(运行时间过长的查询可能是资源匮乏的尝试)。
修复建议：	建议log_duration选项开启:alter system set log_duration ='on';

2.2.8 中风险 确保log_connections选项开启	返回漏洞检测结果
检测项ID：	DBSEC_20181125_16
CVE：	
漏洞类型：	配置缺陷

描述：	该检测项确保log_connections选项开启。启用log_checkpoint设置将导致检查点和重启点被记录在服务器日志中。日志消息中包含一些统计信息，包括写入缓冲区的数量和花费在这些缓冲区上的时间。只有启用这些记录才能确定是否有意外的尝试正在进行中。
修复建议：	建议log_connections选项开启。:alter system set log_connections = 'on';

2.2.9 中风险 确保logging collector开启 返回漏洞检测结果

检测项ID：	DBSEC_20181125_2
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保logging collector开启。logging collector是一个后台进程，用于捕获发送到stderr和的日志消息将它们重定向到日志文件中。 必须启用logging_collector设置才能执行此操作要运行的进程。 它只能在服务器启动时设置。某些类型的logging collector通常比记录到syslog更有用消息可能不会出现在syslog输出中。
修复建议：	建议开启logging collector:alter system set logging_collector = 'on';

2.2.10 中风险 确保SSL正确配置 返回漏洞检测结果

检测项ID：	DBSEC_20181125_23
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保SSL正确配置。如果未正确启用和配置SSL，则会增加数据存在的风险 在运输途中受到损害。
修复建议：	建议开启ssl

2.2.11 低风险 使用了缺省连接端口5432 返回漏洞检测结果

检测项ID：	PGCONFIG011
CVE：	
漏洞类型：	配置缺陷
描述：	检测是否使用了缺省连接端口：5432。 该端口不安全，建议修改为其他端口，以减少被攻击的可能。
修复建议：	建议修改为其他端口。

2.2.12 低风险 检查示例数据库是否删除 返回漏洞检测结果

检测项ID：	DBSEC_20190109_23
CVE：	
漏洞类型：	配置缺陷
描述：	检查示例数据库是否删除。
修复建议：	建议删除示例数据库。

2.2.13 低风险 ALTER USER/CREATE USER设置默认用户密码时没有启用加密 返回漏洞检测结果

检测项ID：	PGCONFIG007
CVE：	
漏洞类型：	配置缺陷
描述：	对于ALTER USER/CREATE USER的密码默认加密功能失效。建议开启该功能。

修复建议：	建议开启密码加密。

2.2.14 低风险 配置了非缺省的 Unix socket 权限	返回漏洞检测结果
检测项ID：	PGCONFIG009
CVE：	
漏洞类型：	配置缺陷
描述：	检测是否配置了非缺省的 Unix socket 权限。
修复建议：	建议该Unix权限配置为 "0511"。重启数据库服务生效

2.2.15 低风险 从PostgreSQL的INFORMATION_SCHEMA.COLUMNS表获取到可能包含密码信息的列	返回漏洞检测结果
检测项ID：	PGDISCO002
CVE：	
漏洞类型：	敏感数据
描述：	INFORMATION_SCHEMA.COLUMNS表可能包含该数据库下其他表的某些信息，如果这些信息中包含敏感数据，可能造成敏感信息泄露。
修复建议：	建议监控对表的访问，并只允许授权用户访问该表/列。由于该表中可能包含业务系统中用户密码信息，建议用户对该表的访问权限进行核查，并使用业务和数据库审计系统审计对该表的访问行为，当该表中内容对外提供时，用户应使用有效的数据脱敏工具或技术对其变形处理

2.2.16 低风险 获取到包含密码的函数和存储过程(Postgresql)	返回漏洞检测结果
检测项ID：	PGPWD003
CVE：	
漏洞类型：	敏感数据
描述：	ROUTINES表包含了存储过程和函数的相关信息。通过它可以获取到包含密码的函数和存储过程。禁止低权限用户访问ROUTINES表，避免敏感信息泄露。
修复建议：	建议只允许授权用户访问该表并监控他们的非授权活动。

2.2.17 低风险 确保log_error_verbosity设置正确	返回漏洞检测结果
检测项ID：	DBSEC_20190109_5
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项确保log_error_verbosity设置正确。log_error_verbosity设置指定的记录的详细程度。如果没有设置为正确的值，可能太多的细节或过少的细节被记录下来，请根据需要设置恰当的值。
修复建议：	建议log_error_verbosity设置为verbose。

2.2.18 注意 确保安装了set_user拓展应用	返回漏洞检测结果
检测项ID：	DBSEC_20190109_24
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查是否安装了set_user拓展应用，该应用用于控制和审计超级用户数据库角色的使用，从而有效阻止非法授权。

修复建议：	建议启用set_user拓展程序。

2.2.19 注意 确保Postmaster运行时参数配置正确 返回漏洞检测结果

检测项ID：	DBSEC_20190109_20
CVE：	
漏洞类型：	配置缺陷
描述：	这些参数的改变将影响数据库服务的运行，参数设置不当将导致拒绝服务以及数据损坏。
修复建议：	请检查当前参数配置是否合理。

2.2.20 注意 确保Superuser运行时参数配置正确 返回漏洞检测结果

检测项ID：	DBSEC_20190109_17
CVE：	
漏洞类型：	配置缺陷
描述：	为改进服务性能数据库超级管理员可对这些参数进行配置。这些参数的恶意篡改将导致服务重启。
修复建议：	这些配置项的修改将会导致服务重启，请检查参数是否被篡改，参数设置是否合理。

2.2.21 注意 确保PostgreSQL配置文件独立于数据簇之外 返回漏洞检测结果

检测项ID：	DBSEC_20190109_27
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查配置文件目录和授权情况。配置文件存在于数据簇目录下，很可能会有意无意的被更改，从安全性考虑，应该独立于数据集群目录；文件访问权限应该仅限于超级用户和授权用户。
修复建议：	建议用户根据当前需要合理规划配置文件的位置，建议独立于数据簇之外；确保文件的访问权限得到限制；在postgresql.conf配置文件中相应地更改设置并重新启动数据库集群更改生效。

2.2.22 注意 检查超级用户权限授予情况 返回漏洞检测结果

检测项ID：	DBSEC_20190109_12
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查超级用户权限被授予给哪些角色,如果有角色不应该被授权请及时收回。
修复建议：	数据库超级用户绕过了除登录以外的所有权限的检查，这是一个不安全的特权，请确认授予的用色是否安全。

2.2.23 注意 检查登录权限授予情况 返回漏洞检测结果

检测项ID：	DBSEC_20190109_13
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查登录权限被授予给哪些角色,如果有角色不应该被授权请及时收回。
修复建议：	请检查用户列表，确认登录权限授予是否合规，对于非法用户请及时收回权限。

2.2.24 注意 检查create db权限授予情况 返回漏洞检测结果

检测项ID：	DBSEC_20190109_15
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查create db权限被授予给哪些角色,如果有角色不应该被授权请及时收回。
修复建议：	请检查用户列表，确认创建数据库权限授予是否合规，对于非法用户请及时收回权限。

2.2.25 注意 确保User运行时参数配置正确 返回漏洞检测结果

检测项ID：	DBSEC_20190109_18
CVE：	
漏洞类型：	配置缺陷
描述：	为了提高性能或者某项特性，用户可以在事务、实体或会话中改变user运行时参数，一旦参数被篡改会存在宕机风险。
修复建议：	请检查当前参数配置是否合理，需要注意的是当前参数修改后必须手动恢复默认值。

2.2.26 注意 确保'backend'运行参数设置正确 返回漏洞检测结果

检测项ID：	DBSEC_20190109_8
CVE：	
漏洞类型：	配置缺陷
描述：	为了有效地服务多个客户端，PostgreSQL服务器为每个客户端"后端"的启动一个新的进程。一个新的子进程后立即创建检测传入的连接。在这个基准测试运行参数控制由后端处理。参数的更改将影响服务器整体运行。
修复建议：	请检查当前参数配置是否合理，需要注意的是当前参数修改后需要重启服务生效。

2.2.27 注意 确保PostgreSQL子目录位置在数据簇之外 返回漏洞检测结果

检测项ID：	DBSEC_20190109_26
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查子目录位置和授权情况。数据库簇在不同子目录下执行特定的任务，性能、可靠性、安全性这些子目录需要重定向在数据集群之外；且当前文件和路径的访问权限应该仅限于超级用户和授权用户。
修复建议：	建议用户根据当前需要，合理设置数据、日志表空间的目录，建议独立于数据簇之外；确保文件的访问权限得到限制；目录移动到其他分区时需要确保空间足够，避免空间利用率过度；在postgresql.conf配置文件中相应地更改设置并重新启动数据库集群更改生效。

2.2.28 注意 确保为流复制创建了专用用户 返回漏洞检测结果

检测项ID：	DBSEC_20190109_25
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查有流复制权限的用户，没有必要使用超级用户账号启动流复制，遵循最小权限的一般原则，应该为流复制创建专门的用户。
修复建议：	建议创建专门的流复制用户。

2.2.29 注意 检查密码有效期设置为永不过期的角色 返回漏洞检测结果

检测项ID：	DBSEC_20190109_11
CVE：	

漏洞类型：	配置缺陷
描述：	该检测项检测密码有效期设置为永不过期的角色，建议设置密码有效期。
修复建议：	建议设置角色密码有效期。

2.2.30 注意 检查create role权限授予情况 返回漏洞检测结果

检测项ID：	DBSEC_20190109_14
CVE：	
漏洞类型：	配置缺陷
描述：	该检测项检查create role权限被授予给哪些角色,如果有角色不应该被授权请及时收回。
修复建议：	请检查用户列表，确认创建角色权限授予是否合规，对于非法用户请及时收回权限。

2.2.31 注意 确保DML权限授予合理 返回漏洞检测结果

检测项ID：	DBSEC_20190109_22
CVE：	
漏洞类型：	配置缺陷
描述：	DML（插入，更新，删除）在表级别的操作，应只限于授权用户。PostgreSQL通过GRANT管理表级DML权限声明。授权不当将导致非法用户修改或删除数据。
修复建议：	请检查用户DML权限授予合理，对于非法用户请及时回收权限。

2.2.32 注意 确保SIGHUP运行时参数配置正确 返回漏洞检测结果

检测项ID：	DBSEC_20190109_19
CVE：	
漏洞类型：	配置缺陷
描述：	为了提高性能或者某项特性，超级用户可以改变这些参数，这些参数设置不当将导致拒绝服务及数据损坏。
修复建议：	建议在PostgreSQL的配置文件恢复所有参数值并调用服务器重新加载配置文件。