### 安全计算环境层面问题和整改建议

#### 服务器和终端

| **关联资产** | **安全层面** | **控制点** | **控制项** | **原始 风险值** | **问题描述** | **问题分析** | **危害分析** | **整改建议** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 交换服务器、数据库系统数据库服务器1、数据库系统应用服务器、遥测综合管控集成服务器、遥测综合管控数据库服务器、遥测综合管控应用服务器、机动车排污监控数据库服务器、机动车排污监控应用服务器、大气监控平台GIS服务器 | 安全计算环境 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | **高** | 服务器、终端未满足口令复杂度校验机制，存在弱口令和相同口令，未定期更换口令。 | 服务器、终端未开启口令强度校验功能，未定期更换管理账户口令，容易产出弱口令引起系统安全性。 | 存在弱口令可能导致被攻击者暴力破解的可能性。 | 1、建议对windows操作系统开启本地安全策略-账户策略-密码策略，启用密码复杂性要求，设置密码最小长度为8个字符； 2、建议对Windows操作系统进行加固，开启本地安全策略-账户策略-密码策略：密码必须符合复杂性要求 已启用，密码长度最小值：8个字符，密码最长使用期限：90天。 |
| 交换服务器、遥测综合管控数据库服务器、遥测综合管控集成服务器、数据库系统应用服务器、数据库系统数据库服务器1、大气监控平台GIS服务器、机动车排污监控应用服务器、机动车排污监控数据库服务器、遥测综合管控应用服务器、大气监控平台备份服务器、大气监控平台模型服务器、大气监控平台应用服务器、大气监控平台数据库服务器 | 安全计算环境 | 身份鉴别 | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | **高** | 操作系统无登录失败处理功能，操作系统未设置超时。 | 操作系统未开启登录失败策略，可输入多次错误口令；操作系统开启设置屏保功能，服务器操作未设置远程超时退出功能。 | 登录口令可能被恶意用户使用暴力猜解方式获得，合法用户身份被仿冒，导致系统被非授权访问。 | 1.建议开启终端Windows操作系统账户策略-账户锁定策略，账户锁定阈值为5次，账户锁定时间为30分钟； 2.建议开启终端Windows操作系统屏幕保护程序，结合业务需求，设置屏保等待时间，如15分钟，并勾选“恢复时显示登录屏幕”。 |
| 交换服务器、数据库系统数据库服务器1、数据库系统应用服务器、遥测综合管控集成服务器、遥测综合管控数据库服务器、大气监控平台数据库服务器、大气监控平台应用服务器、大气监控平台模型服务器、大气监控平台备份服务器、遥测综合管控应用服务器、机动车排污监控数据库服务器、机动车排污监控应用服务器、大气监控平台GIS服务器 | 安全计算环境 | 访问控制 | a）应对登录的用户分配账户和权限； | **中** | 未禁用或限制服务器默认账户的访问权限。 | 未禁用或限制默认账户的访问权限，默认账户（管理员）权限过大，可能导致无法在管理员级别形成权限相互制约，管理员权限过大，可能无法对管理员的行为进行监管、制约 | 未禁用或限制默认账户的访问权限，默认账户（管理员）权限过大，可能导致无法在管理员级别形成权限相互制约，管理员权限过大，可能无法对管理员的行为进行监管、制约 | 建议对服务器默认账户进行限制或禁用。 |
| 交换服务器、遥测综合管控数据库服务器、遥测综合管控集成服务器、数据库系统应用服务器、数据库系统数据库服务器1、大气监控平台GIS服务器、机动车排污监控应用服务器、机动车排污监控数据库服务器、遥测综合管控应用服务器、大气监控平台备份服务器、大气监控平台模型服务器、大气监控平台应用服务器、大气监控平台数据库服务器 | 安全计算环境 | 访问控制 | d）应授予管理用户所需的最小权限，实现管理用户的权限分离。 | **中** | 服务器、终端未对管理员用户进行三权分立，未实现管理用户权限最小化。 | 目前按照最小权限原则分配系统中用户的权限，但系统中无安全审计员角色，未与管理员形成相互制约的关系。未在设备使用手册中要求在分配用户权限时进行权限分离和相互制约。 | 可能导致用户权限过大而滥用的风险。 | 建议将服务器、终端特权用户的权限进行分离，分为审计管理员、安全管理员、系统管理员等权限用户。 |
| 交换服务器、数据库系统数据库服务器1、数据库系统应用服务器 | 安全计算环境 | 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | **高** | 服务器未开启审核策略。 | 操作系统和数据库日志审计功能不完善，未开启审计功能；无法对用户的所有行为等进行日志记录。 | 无法对安全事件进行追溯，同时无法及时了解实际运行状况以及存在的安全隐患。 | 1.建议开启服务器审核功能，如：控制面板-管理工具-安全策略-本地安全策略-审核策略下开启全部审核功能。 |
| 数据库系统应用服务器、数据库系统数据库服务器1、遥测综合管控集成服务器、遥测综合管控数据库服务器、交换服务器、遥测综合管控应用服务器、机动车排污监控数据库服务器、机动车排污监控应用服务器 | 安全计算环境 | 安全审计 | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 | **高** | 服务器、终端、审计记录未上传至日志审计设备中进行集中保护。 | 未上传至日志审计设备中进行集中保护。 | 可能导致安全事件日志被攻击者删除，不能进行事件追溯。 | 建议将服务器、终端审计日志上传至日志审计设备中进行集中保护。 |
| 遥测综合管控数据库服务器、遥测综合管控集成服务器、大气监控平台GIS服务器、遥测综合管控应用服务器、大气监控平台数据库服务器、大气监控平台应用服务器、大气监控平台模型服务器、大气监控平台备份服务器 | 安全计算环境 | 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | **高** | 操作系统未最小化安装。 | 操作系统未最小化安装，安装了与业务无关的应用程序，如：向日葵。 | 应用程序可能存在安全漏洞，或影响操作系统性能，造成业务中断。 | 建议加强操作系统的管理，卸载或禁用多余的组件、服务和应用程序。 |
| 大气监控平台备份服务器、大气监控平台模型服务器、大气监控平台应用服务器、大气监控平台数据库服务器、遥测综合管控应用服务器、机动车排污监控数据库服务器、大气监控平台GIS服务器、机动车排污监控应用服务器、遥测综合管控集成服务器、遥测综合管控数据库服务器、数据库系统数据库服务器1、数据库系统应用服务器、交换服务器 | 安全计算环境 | 入侵防范 | b）应关闭不需要的系统服务、默认共享和高危端口； | **高** | 服务器开启了135 、137、445等高危端口及默认共享。 | 服务器开启了不需要的服务、磁盘共享和高危端口。如：开启了135 、137、445等高危端口。 | 多余的服务、共享和端口可能被恶意者利用和攻击，造成系统崩溃，引起系统安全。 | 建议加强服务器的管理，禁用不需要的服务；通过注册表关闭磁盘默认共享；通过系统防火墙或IP安全策略设置策略禁用高危端口通信。 |
| 机动车排污监控应用服务器、机动车排污监控数据库服务器 | 安全计算环境 | 恶意代码防范 | a）应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。 | **中** | 未安装防病毒软件 | 操作系统未安装防病毒软件。 | 缺乏统一的病毒监控机制将不利于管理员掌握系统内各主机操作系统的病毒防护现状，无法在病毒暴发时采取及时的应对措施。 | 建议部署网络恶意代码防护产品和主机防病毒软件，并通过病毒监控中心对服务器病毒感染情况进行监控。定期更新防病毒软件特征库降低主机感染病毒、木马的风险。 |
| 机动车排污监控数据库服务器、机动车排污监控应用服务器、大气监控平台GIS服务器、大气监控平台数据库服务器、大气监控平台应用服务器、大气监控平台模型服务器、大气监控平台备份服务器、交换服务器、数据库系统应用服务器、数据库系统数据库服务器1 | 安全计算环境 | 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | **中** | 操作系统未对计算设备进行可信验证。 | 操作系统未对计算设备和应用软件的系统引导程序、系统程序、重要配置参数和应用程序进行可信验证。 | 系统引导程序、系统程序、重要配置参数和应用程序以及应用程序的关键执行环节均可能存在被篡改的风险，导致系统和程序被未授权访问。 | 建议部署可信验证系统，对系统的引导，程序启动和运行过程进行可信验证，并对可信验证遭到破坏时进行告警和分析。 |
| 大气监控平台备份服务器、大气监控平台模型服务器、大气监控平台应用服务器、大气监控平台数据库服务器、大气监控平台GIS服务器、机动车排污监控应用服务器、机动车排污监控数据库服务器 | 安全计算环境 | 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | **中** | 未对服务器配置数据进行本地备份和恢复测试。 | 管理员未对系统的数据每天进行完全备份。 | 系统如出现故障，可能无法及时恢复，或造成重要数据丢失。 | 建议对数据每天至少完全备份一次，并将备份介质场外存放，此外，还应定期对备份文件进行恢复测试，确保备份文件有效。 |
| 机动车排污监控数据库服务器、遥测综合管控应用服务器、机动车排污监控应用服务器、大气监控平台GIS服务器、大气监控平台数据库服务器、大气监控平台应用服务器、大气监控平台模型服务器、大气监控平台备份服务器、交换服务器、数据库系统数据库服务器1、数据库系统应用服务器、遥测综合管控数据库服务器、遥测综合管控集成服务器 | 安全计算环境 | 数据备份恢复 | b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 | **中** | 服务器、终端未提供异地数据备份功能。 | 备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。 | 如机房遭受严重破坏，可能导致数据完全丢失。 | 建议利用通信网络将关键数据定时批量传送至备用场地，实现数据异地备份。 |
| 交换服务器、遥测综合管控集成服务器、遥测综合管控数据库服务器、数据库系统应用服务器、数据库系统数据库服务器1、大气监控平台备份服务器、大气监控平台模型服务器、大气监控平台应用服务器、大气监控平台数据库服务器、大气监控平台GIS服务器、机动车排污监控应用服务器、遥测综合管控应用服务器、机动车排污监控数据库服务器 | 安全计算环境 | 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。 | **中** | Windows操作系统剩余信息释放机制不完善。 | Windows操作系统剩余信息保障不完善。 | 可能被未授权人员获取相关信息，导致信息泄露。 | 建议设置Windows操作系统本地安全策略-本地策略-安全选项： 启用“交互式登录：不显示最后的用户名”。 |

#### 应用系统和数据库

| **关联资产** | **安全层面** | **控制点** | **控制项** | **风险值** | **问题描述** | **问题分析** | **危害分析** | **整改建议** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 大气监控平台、机动车排污监控系统、怀化遥测综合管控平台系统、重点排污单位自动监控与基础数据库系统、SQL Server数据库、MySQL数据库、Oracle数据库 | 安全计算环境 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | **高** | 数据库、应用系统未满足口令复杂度校验机制，存在弱口令和相同口令，未定期更换口令。 | 数据库、应用系统未开启口令强度校验功能，未定期更换管理账户口令，容易产出弱口令引起系统安全性。 | 存在弱口令可能导致被攻击者暴力破解的可能性。 | 1、建议开启Oracle数据库“PASSWORD\_VERIFY\_FUNCTION ”函数，设置口令强度策略，或使用第三方加固系统加固； 2、建议对SQLServer数据库所在Windows服务器操作系统进行加固； 3、建议在应用系统加入密码复杂度校验机制，如口令长度≥8，由大小写、数字和特殊字符其中三类组成（最低要求：长度大于6，由字母和数字组成）； 4、建议每90天定期更换操作系统、数据库和应用系统管理账户的口令。 3、建议开启MySQL数据库“validate password”插件，设置口令强度策略。 |
| 重点排污单位自动监控与基础数据库系统、机动车排污监控系统、大气监控平台、怀化遥测综合管控平台系统SQL Server数据库、Oracle数据库、MySQL数据库 | 安全计算环境 | 身份鉴别 | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | **高** | 数据库、应用系统无登录失败处理功能，操作系统未设置超时。 | 数据库、应用系统未开启登录失败策略，可输入多次错误口令；操作系统开启设置屏保功能，服务器操作未设置远程超时退出功能。 | 登录口令可能被恶意用户使用暴力猜解方式获得，合法用户身份被仿冒，导致系统被非授权访问。 | 1、建议对部署数据库的服务器设置登录失败处理功能和空闲会话超时自动退出操作界面； 2、建议对应用系统设置登录失败处理机制，如登录失败5次，锁定该账户10分钟。 |
| 大气监控平台、机动车排污监控系统、重点排污单位自动监控与基础数据库系统、怀化遥测综合管控平台系统 | 安全计算环境 | 身份鉴别 | c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 | **高** | 应用系统远程管理时采用http登陆管理，数据明文传输，未采用加密技术防止鉴别信息在网络传输过程中被窃听。 | 应用系统在进行远程管理时未采取必要措施，防止鉴别信息在网络传输过程中被窃听。 | 应用系统帐号、口令等重要数据可能被嗅探并盗用，导致应用系统被非授权访问。 | 建议应用系统采取外部加密机制或采用https登录方式，防止鉴别信息在网络传输过程中被窃听。 |
| 怀化遥测综合管控平台系统、重点排污单位自动监控与基础数据库系统、机动车排污监控系统、大气监控平台、交换SQL Server数据库、MySQL数据库、Oracle数据库 | 安全计算环境 | 访问控制 | a）应对登录的用户分配账户和权限； | **中** | 未禁用或限制数据库、应用系统默认账户的访问权限。 | 未禁用或限制默认账户的访问权限，默认账户（管理员）权限过大，可能导致无法在管理员级别形成权限相互制约，管理员权限过大，可能无法对管理员的行为进行监管、制约 | 未禁用或限制默认账户的访问权限，默认账户（管理员）权限过大，可能导致无法在管理员级别形成权限相互制约，管理员权限过大，可能无法对管理员的行为进行监管、制约 | 建议对数据库、应用系统默认账户进行限制或禁用。 |
| 大气监控平台、机动车排污监控系统、重点排污单位自动监控与基础数据库系统、怀化遥测综合管控平台系统、SQL Server数据库、Oracle数据库、MySQL数据库 | 安全计算环境 | 访问控制 | d）应授予管理用户所需的最小权限，实现管理用户的权限分离。 | **中** | 数据库、应用系统未对管理员用户进行三权分立，未实现管理用户权限最小化。 | 目前按照最小权限原则分配系统中用户的权限，但系统中无安全审计员角色，未与管理员形成相互制约的关系。未在设备使用手册中要求在分配用户权限时进行权限分离和相互制约。 | 可能导致用户权限过大而滥用的风险。 | 建议将数据库、应用系统特权用户的权限进行分离，分为审计管理员、安全管理员、系统管理员等权限用户。 |
| SQL Server数据库、MySQL数据库、Oracle数据库 | 安全计算环境 | 安全审计 | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 | **高** | 数据库审计记录未上传至日志审计设备中进行集中保护。 | 未上传至日志审计设备中进行集中保护。 | 可能导致安全事件日志被攻击者删除，不能进行事件追溯。 | 建议将数据库审计日志上传至日志审计设备中进行集中保护。 |
| 怀化遥测综合管控平台系统、重点排污单位自动监控与基础数据库系统、机动车排污监控系统、大气监控平台、SQL Server数据库、Oracle数据库、MySQL数据库 | 安全计算环境 | 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | **中** | 操作系统、中间件、数据库和应用系统未对计算设备进行可信验证。 | 操作系统、中间件、数据库和应用系统未对计算设备和应用软件的系统引导程序、系统程序、重要配置参数和应用程序进行可信验证。 | 系统引导程序、系统程序、重要配置参数和应用程序以及应用程序的关键执行环节均可能存在被篡改的风险，导致系统和程序被未授权访问。 | 建议部署可信验证系统，对系统的引导，程序启动和运行过程进行可信验证，并对可信验证遭到破坏时进行告警和分析。 |
| 大气监控平台、机动车排污监控系统、重点排污单位自动监控与基础数据库系统、怀化遥测综合管控平台系统 | 安全计算环境 | 数据完整性 | a）应采用校验技术保证重要数据在传输过程中的完整性。 | **高** | 未采用密码技术进行通信完整性验证。 | 未采用密码技术保证通信过程中数据的完整性。 | 可能导致重要数据在传输过程中被攻击者劫持、篡改。 | 建议为业务应用系统配置SSL证书/HTTPS证书。 |
| 大气监控平台、大气监控平台GIS服务器、机动车排污监控应用服务器、机动车排污监控数据库服务器、大气监控平台备份服务器、大气监控平台模型服务器、大气监控平台应用服务器、大气监控平台数据库服务器 | 安全计算环境 | 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | **中** | 未对服务器配置数据和应用系统的业务数据、数据库数据进行本地备份和恢复测试。 | 管理员未对系统的数据每天进行完全备份。 | 系统如出现故障，可能无法及时恢复，或造成重要数据丢失。 | 建议对数据每天至少完全备份一次，并将备份介质场外存放，此外，还应定期对备份文件进行恢复测试，确保备份文件有效。 |
| 大气监控平台、机动车排污监控系统、怀化遥测综合管控平台系统、重点排污单位自动监控与基础数据库系统、SQL Server数据库、MySQL数据库、Oracle数据库 | 安全计算环境 | 数据备份恢复 | b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 | **中** | 数据库、应用系统未提供异地数据备份功能。 | 备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。 | 如机房遭受严重破坏，可能导致数据完全丢失。 | 建议利用通信网络将关键数据定时批量传送至备用场地，实现数据异地备份。 |
| 重点排污单位自动监控与基础数据库系统、怀化遥测综合管控平台系统、机动车排污监控系统、大气监控平台、SQL Server数据库、Oracle数据库、MySQL数据库 | 安全计算环境 | 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | **高** | 单位未制定公民个人信息在信息系统收集中的相关管理制度。 | 对信息系统收集用户的个人信息未制定管理相关制度。 | 无相关制度管理收集的个人信息，可能因漏洞或恶意攻击导致用户的个人信息泄露，影响单位信誉，引起经济损失。 | 建议结合行业或主管部门相关法律法规制定个人信息管理流程或制度，对应用系统所需的个人信息的收集、使用、存储和授权等方面进行规范化管理。 |
| 大气监控平台、机动车排污监控系统、怀化遥测综合管控平台系统、重点排污单位自动监控与基础数据库系统、Oracle数据库、SQL Server数据库、MySQL数据库 | 安全计算环境 | 个人信息保护 | b）应禁止未授权访问和非法使用用户个人信息。 | **高** | 单位内部未制定对个人信息进行保护的相关管理制度。 | 对系统内收集用户的个人信息未制定管理相关制度。 | 无相关制度管理收集的个人信息，可能因漏洞或恶意攻击导致用户的个人信息泄露，影响单位信誉，引起经济损失。 | 建议结合行业或主管部门相关法律法规制定个人信息管理流程或制度，对应用系统所需的个人信息的收集、使用、存储和授权等方面进行规范化管理。 |

# 建议部署测评清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **硬件/软件** | **数量** | **整改说明** |
| 无 | | | | |

【全文结束】