**xxxxxxx管理系统**

**安全加固报告**

# 概述

## 目的

对xxxxxxxx管理系统所在的主机、防火墙和交换机进行安全检查，了解自身系统所存在的安全问题及风险，对系统的配置进行分析和检查，按照等级保护三级技术要求进行分析，对存在安全风险的系统配置进行安全加固，以满足等级保护相关要求。

## 遵循规范

安全加固遵循《信息安全技术 信息系统安全等级保护基本要求》标准，按照三级系统的技术要求，从身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码审计和资源控制7个方面面进行安全检查，对检查中的不满足项进行安全加固。

## 检查方法

通过控制台审计对设备进行本地操作，提取系统的配置情况来了解系统的安全状况，因而可以更全面地了解系统的安全现状，对扫描结果进行验证，弥补漏洞扫描的不足，使得评估结果更准确，更加真实。

## 加固范围

|  |  |  |
| --- | --- | --- |
| **资产名称** | **产品型号** | **IP地址** |
| 数据库服务器 | linux | xx.xx.xx.41 |
| 数据库服务器 | linux | xx.xx.xx.42 |
| 银行接口服务器 | Red hat linux | xx.xx.xx.50 |
| 银行接口服务器 | Red hat linux | xx.xx.xx.52 |
| 签名服务器 | Red hat linux | xx.xx.xx.49 |
| 签名服务器 | Red hat linux | xx.xx.xx.49 |
| 应用服务器 | Red hat linux | xx.xx.xx.45 |
| 应用服务器 | Red hat linux | xx.xx.xx.46 |
| 应用服务器 | Red hat linux | xx.xx.xx.47 |
| 应用服务器 | Red hat linux | xx.xx.xx.48 |
| 应用服务器 | Red hat linux | xx.xx.xx.53 |
| 应用服务器 | Red hat linux | xx.xx.xx.54 |
| 防火墙 | 东软 |  |
| 交换机 | H3C |  |

# 安全加固

## 主机安全加固

### 认证授权

#### 禁用不需要的帐号

|  |  |
| --- | --- |
| **安全要求** | 系统中不存在未授权的用户 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 系统存在games、ftp系统账号 |
| **是否满足要求** | 不满足 |
| **是否加固** | 加固 |
| **加固内容** | 禁用games和ftp账号，银行接口服务器需要使用ftp账号，不能禁用。  数据库存在bs、fj、fjtest、fs、fstest五个测试账号，建议删除。  银行接口服务器应用系统需要ftp账号，账号保留。 |
| **备注** | oracle数据库中存在测试账号，账号为bs、fj、fjtest、fs、fstest，需要集成商确认后删除账号 |

#### 设置严格的密码策略

|  |  |
| --- | --- |
| **安全要求** | 口令长度不小于8个字符，口令有效期90天，设置登陆失败5次账户锁定，锁定时间300秒，设置口令的复杂度。 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** |  |
| **是否满足要求** | 不满足 |
| **是否加固** | 加固 |
| **加固内容** |  |

#### 启用账户超时锁定策略

|  |  |
| --- | --- |
| **安全要求** | 10分钟无任何操作，自动退出登录 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 默认超时时间为1000秒 |
| **是否满足要求** | 不满足 |
| **是否加固** | 加固 |
| **加固内容** | 修改超时时间为600秒  ***TMOUT=600*** |

#### 系统登陆限制

|  |  |
| --- | --- |
| **安全要求** | 设置登陆失败5次账户锁定，锁定时间300秒。 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 系统没有启用登录失败锁定功能 |
| **是否满足要求** | 不满足 |
| **是否加固** | 暂时未加固 |
| **加固方法** | 以root管理员身份登录系统，输入以下命令：  1、修改策略文件  ***vi /etc/pam.d/system-auth***  检查文件中是否存在：  account required /bin/security/pam\_tally.so deny= |
| **备注** | 由于管理员无法确定该策略加固后是否对应用系统构成影响，暂时未加固。 |

#### 限制root登陆的控制台

|  |  |
| --- | --- |
| **安全要求** | 限制root只能从tty1、tty2控制台登录 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** |  |
| **是否满足要求** | 不满足 |
| **是否加固** | 加固 |
| **加固内容** | 修改只能通过tty1和tty2控制台登录 |

#### 系统只存在一个超级用户

|  |  |
| --- | --- |
| **安全要求** | 检查系统中的超级用户数量，建议只保留一个有系统管理员权限的超级用户；查看是否有管理员不知道的超级用户。 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 只有一个超级用户 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 每个用户都应当设置口令，并且口令被屏蔽（shadowed）

|  |  |
| --- | --- |
| **安全要求** | 系统中的每个用户都应当设置口令，并且口令使用shadow方式加密 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 口令已经进行加密 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

### 文件目录访问控制

#### 检查passwd、shadow、group和gshadow文件权限

|  |  |
| --- | --- |
| **安全要求** | 对系统的重要文件和目录设置适当的权限：  /etc/passwd 所有用户可读，root可写；  /etc/shadow 只有root可读  /etc/group 所有用户可读，root可写；  /etc/gshadow只有root可读 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 文件只有root可读 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 限制具有SUID权限标志的程序

|  |  |
| --- | --- |
| **安全要求** | 限制具有SUID/SGID权限的程序，系统中不存在未授权的SUID/SGID可执行文件 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 经过与管理员确认，系统中不存在未授权的可执行文件。 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 设置umask为022

|  |  |
| --- | --- |
| **安全要求** | 设置用户的umask为022，即所有者完全控制，组内用户和其他用户只允许读取和执行。 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 默认掩码是022 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### root 用户环境变量的安全性

|  |  |
| --- | --- |
| **安全要求** | root环境变量中不包含当前目录。 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 环境变量中不包含当前目录 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 删除中没无属主的文件

|  |  |
| --- | --- |
| **安全要求** | 系统中不存在无属主的文件和目录 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 系统中存在一些临时文件，跟管理确认属于系统正常文件，无法删除 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 删除系统中异常隐含的文件

|  |  |
| --- | --- |
| **安全要求** | 系统中没有异常的隐藏文件 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 系统中无异常的文件，是应用程序正常的文件 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

### 入侵防范

#### 关闭不需要的系统服务

|  |  |
| --- | --- |
| **安全要求** | 关闭无效的服务，提高系统性能，增加系统安全性。  禁止下列不必要的基本网络服务。  ftp, telnet, talk, ntalk, imap, pop-2, pop-3, finger, sendmail |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 系统开发人员无法确认需哪些服务，此项工作内容带确定 |
| **是否满足要求** | 不满足 |
| **是否加固** | 暂时不加固 |
| **加固内容** | 无 |
| **备注** | 集成商无法确定哪些服务对应用系统有影响，待后期确定后在加固。 |

#### SSH方式远程管理，限制远程登录的网段

|  |  |
| --- | --- |
| **安全要求** | 限制只运行固定网段管理和维护系统 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 登陆服务器只能到机房登陆，登陆网段已经做限制 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

### 安全审计

#### 使用syslog记录系统日志配置

|  |  |
| --- | --- |
| **安全要求** | 启用syslog日志服务，或者使用集中日志管理系统 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 启用了日志服务器记录日志，日志本地保存，后期会上日志管理系统。 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 合理设置Syslog日志记录级别

|  |  |
| --- | --- |
| **安全要求** | 系统记录登录失败、系统报错等日志信息。 |
| **配置现状** | 系统记录所以的登陆日志，保存信息。 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 本地日志存放非系统目录，只有root用户可删除

|  |  |
| --- | --- |
| **安全要求** | 系统日志记录的目录和文件权限配置合理，只有root用户可删除。 |
| **检查对象** | Web前端及应用服务器6台：  xx.xx.xx.35、xx.xx.xx.46、xx.xx.xx.47、xx.xx.xx.48、xx.xx.xx.53、xx.xx.xx.54  签名服务器2台：  xx.xx.xx.45、xx.xx.xx.50（地址冲突，待确定）  银行接口服务器2台：  xx.xx.xx.51、xx.xx.xx.50  数据库服务器2台：  xx.xx.xx.41、xx.xx.xx.42 |
| **配置现状** | 日志只有root用户可删除 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

## 防火墙及交换机安全加固

### 访问控制

#### 边界控制

|  |  |
| --- | --- |
| **安全要求** | 在网络边界部署访问控制设备，启用访问控制功能。 |
| **检查对象** | 防火墙和交换机 |
| **配置现状** | 网络出口出部署防火墙、负载均衡设备对互联网进行隔离。 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 策略检查

|  |  |
| --- | --- |
| **安全要求** | 为数据流提供明确的允许/拒绝访问的能力，访问控制策略为端口级。 |
| **检查对象** | 防火墙 |
| **配置现状** | 防火墙测试中设置了从互联网访问票据系统的IN/OUT两条策略，票据系统仅对互联网开放业务端口。 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 应用层过滤措施

|  |  |
| --- | --- |
| **安全要求** | 对网络的内容进行过滤，实现对应用层协议HTTP、telnet、smtp等协议的控制。 |
| **检查对象** | 防火墙 |
| **配置现状** | 防火墙没有内容过滤的功能，无法对http协议进行审计。 |
| **是否满足要求** | 不满足 |
| **是否加固** | 不加固 |
| **加固内容** | 需要部署应用审计的设备，或者在负载均衡上增加应用审计模块。 |

#### 限制具有拨号访问权限的用户

|  |  |
| --- | --- |
| **安全要求** | 限制使用VPN或者通过其他方式接入单位内网的用户。 |
| **检查对象** | 防火墙、交换机 |
| **配置现状** | 网络中没有使用VPN进行远程管理。 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

### 安全审计

#### 日志功能启用

|  |  |
| --- | --- |
| **安全要求** | 为了对网络设备的运行情况、网络流量、管理记录等进行检测及记录，需要启用系统日志功能。 |
| **检查对象** | 防火墙、交换机 |
| **配置现状** | 系统没有启用日志功能 |
| **是否满足要求** | 不满足 |
| **是否加固** | 不加固 |
| **加固内容** | 计划部署日志管理系统对日志进行集中管理。 |

#### 日志集中管理

|  |  |
| --- | --- |
| **安全要求** | 对日志通过集中管理，防止受到未预期的删除、修改和覆盖等。 |
| **检查对象** | 防火墙、交换机 |
| **配置现状** | 系统没有启用日志功能 |
| **是否满足要求** | 不满足 |
| **是否加固** | 不加固 |
| **加固内容** | 计划部署日志管理系统对日志进行集中管理。 |

### 网络设备防护

#### 禁用不需要的系统账号

|  |  |
| --- | --- |
| **安全要求** | 对登录网络设备的用户进行身份鉴别，系统中不存在非授权的账号。 |
| **检查对象** | 防火墙、交换机 |
| **配置现状** | 系统中只有admin等管理用户，未发现非授权的账号。 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |

#### 密码策略

|  |  |
| --- | --- |
| **安全要求** | 系统使用强壮的密码，密码定期修改。 |
| **检查对象** | 防火墙、交换机。 |
| **配置现状** | 交换机的控制口未设置密码。 |
| **是否满足要求** | 不满足 |
| **是否加固** | 加固 |
| **加固内容** | 修改交换机的口令 |

#### 限制登录设备的地址

|  |  |
| --- | --- |
| **安全要求** | 为了保证网络设备的安全，避免未授权的访问，需要对远程管理的登录地址进行限制。 |
| **检查对象** | 防火墙、交换机 |
| **配置现状** | 票据系统网络环境使用于办公网进行隔离，登录网络设备必须到机房。 |
| **是否满足要求** | 满足 |
| **是否加固** | 不加固 |
| **加固内容** | 无 |