CentOS 操作系统
安全配置规范

龙岗区大数据管理局

2019 年 1 月 21 日

制作人	谢志超、潘一乐、温福城
审核人	张韶君
版本编号	SEC-2019-CENTOS-V1

安全配置要求

1.1 超时自动退出策略

项目编号	SEC-2019-CENTOS-01-01-v1
配置说明	应配置账户超时自动退出策略
配置指南	**1、参考配置** 编辑文件/etc/profile，在文本最后一行添加“export TMOUT=600” **2、补充说明** 参数 600 为 10 分钟，超时退出建议配置在十分钟以内。
检测方法及判定依据	使用 SSH 登录服务器，在预设定时间内无操作，系统会强制登出
回退措施	编辑文件/etc/profile，删除“export =TMOUT XXX”配置
备注	

1.2 用户目录缺省访问权限策略

项目编号	SEC-2019-CENTOS-01-02-v1
配置说明	应设置用户目录缺省访问权限设置
配置指南	**1、参考配置** 编辑文件/etc/login.defs，找到 UMASK 参数，更改其参数值为 027。 **2、补充说明**

检测方法及判定依据	
回退措施	编辑文件/etc/login.defs，找到 UMASK 参数，更改其参数值为修改之前的参数（默认为 077）。
备注	

1.3 密码策略

项目编号	SEC-2019-CENTOS-01-03-v1
配置说明	应设置密码策略
配置指南	**1、参考配置** 编辑文件/etc/login.defs，修改如下参数配置： a.设置密码更改最小间隔天数参数“PASS_MIN_DAYS”值为 2； b.设置密码最小长度参数“PASS_MIN_LEN”值为 6； c.设置密码过期前的警告天数参数“PASS_WARN_AGE”值为 7； d.设置密码最长使用时间参数“PASS_MAX_DAYS”值为 90； **2、补充说明**
检测方法及判定依据	

回退措施	
备注	

1.4 密码复杂度配置

项目编号	SEC-2019-CENTOS-01-04-v1
配置说明	应设置密码复杂度配置
配置指南	**1、参考配置** 编辑文件/etc/pam.d/system-auth，修改如下参数配置： a.设置密码重复使用次数限制，在password sufficient 这一行后追加 remember=5 b.设置密码中的小写字母个数，在password sufficient 这一行后追加 lcredit=-1 c.设置密码中的数字个数，在password sufficient 这一行后追加 dcredit=-1 d.设置密码中的大写字母个数，在password sufficient 这一行后追加 ucredit=-1 e.设置密码中的大写字母个数，在password sufficient 这一行后追加 ocredit=-1 **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.5 远程登录锁定策略

项目编号	SEC-2019-CENTOS-01-05-v1
配置说明	设置远程登录锁定机制
配置指南	**1、参考配置** 在文件/etc/pam.d/system-auth 中，配置 auth required pam_tally2.so deny=5 unlock_time=300 no_lock_time account required pam_tally2.so **2、补充说明** deny=5，为失败次数，unlock_time=300，为锁定时长 300 秒。 在 CentOS 6.5 以前，模块为 pam_tally.so。
检测方法及判定依据	连续五次使用错误用户密码，在使用正确账户密码无法登陆系统，需要等待五分钟之后才能登陆成功
回退措施	
备注	

1.6 设置目录 /tmp/权限

项目编号	SEC-2019-CENTOS-01-06-v1
配置说明	应设置/tmp 目录权限
配置指南	**1、参考配置**

	将目录/tmp/的权限设置为 750 **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.7 删除系统中潜在的危险文件 hosts.equiv 文件

项目编号	SEC-2019-CENTOS-01-07-v1
配置说明	应删除系统中潜在的危险文件 hosts.equiv 文件
配置指南	**1、参考配置** a.执行命令 find / -maxdepth 2 -type f -name hosts.equiv 2>/dev/null 2.进入到 hosts.equiv 文件存在的目录 3.执行命令：rm -fr hosts.equiv **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.8 删除系统中潜在的危险文件.rhosts 文件

项目编号	SEC-2019-CENTOS-01-08-v1

配置说明	删除系统中潜在的危险文件.rhosts 文件
配置指南	**1、参考配置** a.执行命令 find / -maxdepth 3 -type f -name .rhosts 2>/dev/null b.进入到.rhosts 文件存在的目录 c.执行命令：rm -fr .rhosts **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.9 禁用 root 用户远程登录

项目编号	SEC-2019-CENTOS-01-09-v1
配置说明	应禁用 root 用户远程登录
配置指南	**1、参考配置** a.在禁用之前，先增加一个用于远程用户，并查看新增的用户 uid 值，cat /etc/passwd，找到对应用户 UID 值，在/etc/pam.d/system-auth 文件中，找到对应 UID 范围，更改 uid 值，account sufficient pam_succeed_if.so uid < 1000 quiet 确保当前用户 uid 值在范围以内 b.修改/etc/ssh/sshd_config 文件,配置

	PermitRootLogin no，并新增一行 AllowUsers user（user 为新增的用于远程用户）重启服务，/etc/init.d/sshd restart。 **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.10 禁止匿名 VSFTP 用户登陆

项目编号	SEC-2019-CENTOS-01-10-v1
配置说明	禁止匿名 VSFTP 用户登陆
配置指南	**1、参考配置** 编辑/etc/vsftpd.conf(或/etc/vsftpd/vsftpd.conf)文件，设置：anonymous_enable=NO **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.11 禁止 root 用户远程 Telnet 登录

项目编号	SEC-2019-CENTOS-01-11-v1
配置说明	禁止 root 用户远程 Telnet 登录
配置指南	**1、参考配置** 编辑 /etc/pam.d/login 文件，配置 auth required pam_securetty.so **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.12 开启系统防火墙

项目编号	SEC-2019-CENTOS-01-10-v1
配置说明	开启系统防火墙
配置指南	**1、参考配置** a.查看防火墙服务状态 firewall-cmd --state（若服务未开启，则使用 service firewalld start 启动防火墙服务） b.查看防火墙规则 firewall-cmd --list-all，将非必要端口移除（例如：移除 TCP8080 端口 firewall-cmd --permanent --remove-port=8080/tcp） **2、补充说明** 开启之前，需要将业务端口开放（例如：开放业

	务 TCP80 端口 firewall-cmd --permanent --add-port=80/tcp）
检测方法及判定依据	
回退措施	
备注	