1. 金蝶中间件

| **控制点** | **测评项** | **结果记录** | **整改建议** | **备注** |  **整改说明** |
| --- | --- | --- | --- | --- | --- |
| 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； | 1、用户登录中间件管理控制台需要使用账户名和口令；2、用户身份标识唯一，不能新建同名账户；3、未配置口令复杂度检查功能和口令过期更换时间；4、当前账户口令长度均至少8位，包含数字、字母和特殊字符。 | 建议中间件配置口令复杂度检查功能和口令过期更换时间，如用户设置口令时强制要求口令最小长度为8位，字符策略为至少包含1个字母、1个数字和1个特殊字符，设置口令过期更换时间为90天。 | 高风险 | 1）secure用户登录金蝶管控(密码XXX )，点击“系统管理”，默认密码长度时8位，无须修改；密码复杂度选择“复杂”，即口令必须包含字母、数字和特殊字符。2）密码有效天数默认是30天，改为90天3）点击保存按钮 |
| 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； | 未配置登录失败处理功能，未配置登录连接超时自动退出时间。 | 建议中间件配置登录失败处理功能，如设置连续登录失败5次锁定账户15分钟；配置登录连接超时自动退出时间为15分钟。 | 高风险 | 1. 可以使用secure用户（密码XXX）登录，点击“系统管理”，查看：密码重试次数默认为5；用户锁定时间为默认15分钟。管控平台默认会话有效时间默认是30分钟，secure用户登录后，将会话有效时间改为900秒（15分钟），2) admin用户登录（密码XXX），点击“域”-“应用程序配置”-“管理会话超时”，设置时间为15分钟

3）可以连续5次输入错误密码，验证是否锁定15分钟。4）持续15分钟不操作，15分钟后刷新下退出需要登录。 |
| 身份鉴别 | d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 中间件未采用两种或两种以上鉴别技术对用户身份进行鉴别。 | 建议对中间件采用两种或两种以上组合的鉴别技术实现用户身份鉴别，如口令、数字证书、Ukey、令牌、指纹等，其中至少一种鉴别技术应使用密码技术实现。 | 中风险建议整改 | 金蝶中间件管控采用的是口令鉴别技术+验证码实现用户身份鉴别。是否可以，需要测评人员确认下。 |
| 访问控制 | b) 应重命名或删除默认账户，修改默认账户的默认口令； | 未重命名或删除默认账户admin，已修改默认账户的默认口令。 | 建议重命名中间件的默认账户。 | 中风险建议整改 | 1. 修改

${APUSIC\_HOME}/domains/mydomain/config/admin-keyfile文件，把对应的admin、secure、audit用户名修改为符合要求的用户名即可，例如 |
| 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； | 仅设置了系统管理员账户，未设置安全管理员和审计管理员账户，未实现管理用户的权限分离。 | 建议中间件设置系统管理员、审计管理员、安全管理员账户，并根据最小授权原则设置各账户的权限，禁用超管账户，实现三权分立。 | 中风险建议整改 | 不用整改，金蝶中间件有统管理员、审计管理员、安全管理员账户，可以使用secure（密码XXX）登录，点击“用户管理”，查看用户个数；也可以分别使用admin、secure、audit（密码都是XXX）登录进去查看 |
| 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； | 未启用安全审计功能。 | 建议中间件开启安全审计功能，审计覆盖到每个用户，对用户的登录、操作和重要安全事件进行记录。 | 高风险 | 金蝶中间件有开启安全审计功能；使用audit（密码XXX）登录管控，点击“日志”-“审计日志”，查看审计日志信息，审计覆盖到每个用户，对用户的登录、操作和重要安全事件进行记录。 |
| 安全审计 | b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 未启用安全审计功能。 | 建议审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 | 高风险 | 金蝶中间件有开启安全审计功能；使用audit（密码XXX）登录管控，点击“日志”-“审计日志”，查看审计日志信息，审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 |
| 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； | 未启用安全审计功能，未定期对审计日志进行备份，未配置日志服务器实时收集系统的日志信息。 | 建议每天对中间件日志进行备份，并配置日志服务器或使用第三方日志审计系统对各类日志进行收集和保护，降低日志遭到非授权删除、修改或覆盖的风险，并保证审计日志保存时间至少有6个月。 | 高风险 | 金蝶中间件有开启安全审计功能，能进行审计日志的备份。使用audit（密码XXX）登录管控，点击“系统管理”，日志配置下面，配置了审计日志的备份周期并且审计日志保留时间为6个月。 |
| 入侵防范 | c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 未对中间件的接入方式或登录网络地址范围进行限制。 | 建议限制接入中间件的IP地址范围或接入方式，避免无关用户对设备的访问。 | 高风险 | 以管理员（admin）登录管控，“配置”-> “server-config”-> “虚拟服务器”中的访问控制设置黑白名单 |
| 入侵防范 | e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | 未定期通过漏洞扫描、渗透测试等方式发现可能存在的已知漏洞，但已修复本次等保测评中发现的高危漏洞。 | 建议定期通过漏洞扫描、渗透测试等方式发现可能存在的已知漏洞，并在充分测试评估后及时修复。 | 中风险，建议整改 | 针对这个风险，一般是其他第三方用漏扫工具对中间件或者中间件部署的应用系统进行漏洞扫描以及渗透测试等去发现可能存在的漏洞。针对漏扫的结果进行及时修复。所以这项需要集成商和测评人员确认下是否需要去整改 |
| 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； | 未对中间件的配置文件进行备份，未对备份数据开展恢复测试。 | 建议定期对中间件的配置文件进行备份，并定期开展备份数据的恢复测试，验证备份数据的可用性，并妥善保存恢复测试记录。 | 高风险 | 金蝶中间件有定期对中间件的配置文件进行备份。1. 使用audit（密码XXX）登录管控，点击“系统管理”，业务配置备份，可以设置备份目录和定期备份的周期
2. 可以定期开展备份数据的恢复。

具体操作：1.先将原来金蝶服务停止2.${APUSIC\_HOME}/domains/mydomain/config目录备份一下，比如重命名为config-bak3.然后将备份目录/opt/backup/config 复制到${APUSIC\_HOME}/domains/mydomain目录，然后重启金蝶服务验证恢复数据的可用性 |