【应用安全】浅谈 LINUX 系统 WEBLOGIC 安全配置

文/EmmaDai

0x00 WebLogic 应用介绍

WebLogic 是美国 Oracle 公司出品的一个 application server，确切的说是一个基于 JAVAEE 架构的中间件，WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 Java 应用服务器。将 Java 的动态功能和 Java Enterprise 标准的安全性引入大型网络应用的开发、集成、部署和管理之中。

0x01 为什么要做安全配置

作为 web 中间件的 WebLogic 存在安全配置不恰当导致的安全问题。WebLogic 的默认配置中存在一些安全问题，例如弱密码、未开启 SSL 认证等。因此，安全配置 WebLogic 服务器能有效的减少安全威胁，下面将对 WebLogic 安全配置进行讨论。加固方法以 WebLogic 12 为例。

0x02 如何进行安全配置

1. 以非 root 用户运行 WebLogic

WebLogic 进程的用户应该是非超级用户。查看当前系统的 WebLogic 进程，确认程序启动时使用的身份。禁用超级用户启动 WebLogic。

加固方法：
1) 创建 WebLogic 组： groupadd WebLogic
2) 创建 WebLogic 用户并加入 WebLogic 组： useradd WebLogic -g WebLogic
3) 以 WebLogic 身份启动服务

2. 设置加密协议

对于通过 HTTP 协议进行远程维护的设备，设备应支持使用 HTTPS 等加密协议。

加固方法：
启用 SSL 监听，登录控制台选择 [环境]-->[服务器]-->服务器选择-->[一般信息]，勾选“启用 SSL 监听端口”，保存，激活更改。
修改 SSL 默认监听端口，登录控制台选择[环境]-->[服务器]-->服务器选择-->[一般信息]，设置 SSL 监听端口号(非 7002)，保存，激活更改。
配置 SSL 拒绝日志记录，登录控制台选择 [环境]-->[服务器]-->服务器选择-->[配置]-->[SSL]，点击[高级]，勾选"启用 SSL 拒绝日志记录"，保存，激活更改。配置主机名认证，登录控制台选择 [环境]-->[服务器]-->服务器选择-->[配置]-->[SSL]-->高级,主机名验证选择“BEA 主机名验证”，保存，激活更改。
修改主机名认证器，登录控制台选择[环境]-->[服务器]-->服务器选择-->[配置]-->[SSL]-->高级，定制主机名验证器为空，保存，激活更改。

3. 设置账号锁定策略

对于采用静态口令认证技术的设备， 应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号。

加固方法：
配置失败锁定允许尝试次数，登录控制台选择[安全领域]-->领域选择-->[配置]-->[用户封锁]-->勾选“启用封锁”，把“封锁阀值”设为一个小于等于 6 的值，保存,激活更改。
配置锁定持续时间，登录控制台选择[安全领域]-->领域选择-->[配置]-->[用户封锁]-->勾选“启用封锁”，把“封锁持续时间”设为一个大于等于 30 的值，保存,激活更改。
打开锁定帐号策略，登录控制台选择 [安全领域]-->领域选择-->[配置]-->[用户封锁]-->勾选“启用封锁”，保存，激活更改。
配置锁定重置持续时间登录控制台选择 [安全领域]-->领域选择-->[配置]-->[用户封锁]-->勾选“启用封锁”，封锁重置持续时间：6，保存，激活更改。

4. 更改默认端口

为防止恶意的攻击，使得攻击者难以找到数据库并将其定位，使用 HTTP 协议的设备， 应更改 WebLogic 服务器默认端口。

加固方法：
登录控制台选择[环境]-->[服务器]-->服务器选择-->[配置]-->[一般信息]，勾选“启用监听端口”，并修改默认端口号为非 7001 的数值（例如：8001）。

5. 配置定时登出

对于具备字符交互界面的设备，应支持定时账户自动登出。登出后用户需再次登录才能进入系统。设置 http 超时登出，https 超时登出以及控制台会话超时。

加固方法：
设置 http 超时登出，登录控制台选择 [环境]-->[服务器]-->服务器选择-->[配置]-->[优化]，登录超时设置为不大于 5000 的值，保存，激活更改。
设置 https 超时登出，登录控制台选择 [环境]-->[服务器]-->服务器选择-->[配置]-->[优化]，SSL 登录超时设置为不大于 10000 的值，保存,激活更改。
设置控制台会话超时，登录控制台选择 [域名]-->[配置]-->[一般信息]-->[高级]，修改控制台会话超时为不大于 300 的值，保存，激活更改。

6. 开启日志功能

设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，使用的 IP 地址。

加固方法：
登录控制台选择 [环境]-->[服务器]-->服务器选择-->[日志记录]-->[HTTP]，勾选“启用 HTTP 访问日志文件”，保存，激活更改。

7. 禁用 Send Server header

为防止恶意的攻击，获取更多服务器信息，应该禁止发送服务器标头。

加固方法：
登录控制台选择 [环境]-->[服务器]-->服务器选择-->[协议]-->[HTTP]，取消勾选“发送服务器标头”，保存，激活更改。

8. 运行模式设置为生产模式

WebLogic 有两种工作模式，一种是开发模式，另一种是生产模式。开发模式下，启用了自动部署；生产模式下，关闭了自动部署。

加固方法：
登录控制台选择[域名]-->[配置]-->[常规]，勾选“生产模式”，保存，激活更改。

9. 限制应用服务器 Socket 数量

Sockets 最大打开数目设置不当的话，容易受到拒绝服务攻击，超出操作系统文件描述符限制。

加固方法：
登录控制台选择[环境]-->[服务器]-->服务器选择-->[配置]-->[优化]，修改“最大打开套接字数”为 254 或其它用户设定值，保存，激活更改。

10. 配置默认出错页面

WebLogic 应配置错误页面重定向，URL 地址栏中输入错误地址后，应跳转至指向指定错误页面。

加固方法：
修改<WebLogic_install_dir_path>/server/lib/consoleapp/webapp/WEB-INF/web.xml 文件，添加 web-app/error-page/exception-type 节点。

11. 口令长度设置至少为 8 位

对于采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类。

加固方法：
登录控制台选择[安全领域]-->领域选择-->[提供程序]-->[DefaultAuthenticator]-->[配置]-->[提供程序特定]，在“提供程序特定“里设置“最小口令长度”大于等于 8 ，保存，激活更改。

0x03 总结

对 WebLogic 进行安全配置可以有效的防范一些常见安全问题，按照基线标准做好安全配置能够减少安全事件的发生。国内常见的基线标准有中国信息安全等级保护、电信网和互联网安全防护基线配置要求及检测要求，不同的企业也可以根据自身企业业务制定符合自己企业的安全基线标准。

0x04 参考链接

- 国家信息安全等级保护制度要求

电信网和互联网安全防护基线配置要求及检测要求