|  |
| --- |
| **老男孩信息系统安全配置基线**  **Weblogic中间件分册（初稿）** |
| **版本 V1.0** |

**二○一九年一月**

|  |  |  |  |
| --- | --- | --- | --- |
| ■版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |
| [一. 概述 4](#_Toc408317863)  [1.1适用范围 4](#_Toc408317864)  [1.2规范依据 4](#_Toc408317865)  [1.3实施策略 4](#_Toc408317866)  [二. 安全配置基线标准 5](#_Toc408317867)  [2.1身份鉴别 5](#_Toc408317868)  [2.1.1设置密码复杂度 5](#_Toc408317869)  [2.1.2配置帐号锁定 6](#_Toc408317870)  [2.2访问控制 6](#_Toc408317871)  [2.2.1设置受限帐号启动服务 6](#_Toc408317872)  [2.2.2限制目录列表访问 7](#_Toc408317873)  [2.3安全审计 7](#_Toc408317874)  [2.3.1配置审核登录 7](#_Toc408317875)  [2.4资源控制 8](#_Toc408317876)  [2.4.1设置登录超时 8](#_Toc408317877)  [2.4.2限制应用服务器Socket连接数 8](#_Toc408317878)  [2.5其它安全项 10](#_Toc408317879)  [2.5.1配置错误页面处理 10](#_Toc408317880)  [2.5.2禁用Send Server Header 10](#_Toc408317881)  [2.5.3更改默认运行端口 11](#_Toc408317882)  [2.5.4配置加密协议 11](#_Toc408317883)  [三. 评审与修订 12](#_Toc408317884) |

1. 概述
   1. 适用范围

本配置基线适用于老男孩的Weblogic中间件，主要涉及Weblogic中间件安全配置方面的基本要求，用于指导安全例行工作、新系统入网安全检查等场合。

在未特别说明的情况下，均适用于所有运行Weblogic中间件系统。

* 1. 规范依据

根据老男孩目前Weblogic中间件安全现状，综合参考各信息系统运维部门的意见，结合金融行业等级保护实施指引，制定适合于老男孩的基线配置规范。

主要参考依据如下：

* JR/T0071-2012《金融行业信息系统信息安全等级保护实施指引》（2012年7月发布）
  1. 实施策略

结合网络和信息系统建设情况，考虑安全配置项影响的范围，结合以往工作经验，提出如下安全项目实施策略：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **配置类别** | **安全基线项目名称** | **实施策略** |
| 1 | 身份鉴别 | 设置密码并保证复杂度 | 必须实施 |
| 2 | 身份鉴别 | 配置帐号锁定 | 必须实施 |
| 3 | 访问控制 | 设置受限帐号启动服务 | 必须实施 |
| 4 | 访问控制 | 限制目录列表访问 | 必须实施 |
| 5 | 安全审计 | 配置审核登录 | 必须实施 |
| 6 | 资源控制 | 设置登录超时 | 必须实施 |
| 7 | 资源控制 | 限制应用服务器Socket连接数 | 按需实施 |
| 8 | 其它安全项 | 配置错误页面处理 | 必须实施 |
| 9 | 其它安全项 | 禁用SendServerHeader | 建议实施 |
| 10 | 其它安全项 | 更改默认运行端口 | 建议实施 |
| 11 | 其它安全项 | 配置加密协议 | 按需实施 |

1. 安全配置基线标准
   1. 身份鉴别
      1. 设置密码并保证复杂度

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置密码并保证复杂度（必须实施） |
| **安全基线编号** | 中间件-WebLogic-1 |
| **安全基线项说明** | 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。密码应至少每90天进行更换。 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **1、参考配置操作**  查看WebLogic安装目录下的weblogic.properties配置文件。  检查里面“weblogic.system.minPasswordLen=8”的配置是否符合要求。  **2、补充操作说明**  口令要求：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。且5次以内不得设置相同的口令。密码应至少每90天进行更换。 |
| **检查方法** | 查看WebLogic安装目录下的weblogic.properties配置文件内“weblogic.system.minPasswordLen”参数值是否符合要求。 |
| **依据** | 6.2.1.4 应用安全：身份鉴别（S3）：g) 对于系统自动分配或者预设的强度较弱的初始密码，系统应强制用户首次登录时修改初始密码； |
| **备注** |  |

* + 1. 配置帐号锁定

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置帐号锁定（必须实施） |
| **安全基线编号** | 中间件-WebLogic-2 |
| **安全基线项说明** | 要求设定帐号锁定次数和时间，错误输入密码10次，系统自动锁定，锁定时间5分钟。 |
| **配置方法** | 版本：8.x 9.x 10.x版本  1、参考配置操作  查看以管理员身份登录控制台  1. 点击左侧面板”Security”文件夹，展开”REALM”  2. 点击右侧面板中的”User Lock”标签，配置下面的参数：  Lockout Enabled，Lockout Threshold，Lockout Duration  配置的参数可参考如下设置：  Lockout Enabled=true;  Lockout Threshold=10;  Lockout Duration=5 |
| **检查方法** | 参见配置方法中的文件夹，配置文件的参数如下设置则满足要求：  Lockout Enabled=true;  Lockout Threshold=10;  Lockout Duration=5 |
| **依据** | 6.2.1.4 应用安全：身份鉴别（S3）：d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； |
| **备注** | 依据实际需求配置。 |

* 1. 访问控制
     1. 设置受限帐号启动服务

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置受限帐号启动服务（必须实施） |
| **安全基线编号** | 中间件-WebLogic-3 |
| **安全基线项说明** | 要求限制帐号 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **1、参考配置操作**  查看以管理员身份登录控制台  执行“ps–ef| grep–iweblogic”（没有引号）  回显信息不包含root和nobody。 |
| **检查方法** | 参考配置方法中的命令，回显信息不包含root和nobody则满足要求 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系； |
| **备注** |  |

* + 1. 限制目录列表访问

|  |  |
| --- | --- |
| **安全基线项目名称** | 目录列表访问限制（必须实施） |
| **安全基线编号** | 中间件-WebLogic-4 |
| **安全基线项说明** | 禁止WebLogic列表显示文件 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **参考配置操作**  查看WebLogic安装目录下的weblogic.properties配置文件，  检查weblogic.httpd.indexDirectories=是否设置成*false*。示例如下：  weblogic.httpd.indexDirectories= *false* |
| **检查方法** | 参考配置方法中的文件，检查“weblogic.httpd.indexDirectories”参数值设置是否满足要求（值为false则满足） |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问； |
| **备注** |  |

* 1. 安全审计
     1. 配置审核登录

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置审核登录（必须实施） |
| **安全基线编号** | 中间件-WebLogic-5 |
| **安全基线项说明** | 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帐号，登录是否成功，登录时间，以及远程登录时，用户使用的IP地址。 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **参考配置操作**  查看WebLogic安装目录下的weblogic.properties配置文件  开启日志，配置按日期rotate，示例如下：  weblogic.system.enableReverseDNSLookups=*true* |
| **检查方法** | 按配置方法检查“weblogic.system.enableReverseDNSLookups”参数值是否为true，若为true则满足。 |
| **依据** | 6.2.1.4 应用安全：安全审计（G3）：a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计； |
| **备注** |  |

* 1. 资源控制
     1. 设置登录超时

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置登录超时（必须实施） |
| **安全基线编号** | 中间件-WebLogic-6 |
| **安全基线项说明** | 应支持账户登录超时锁定功能。超时后用户需再次输入密码登录才能进入系统。 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **1、参考配置操作**  查看WebLogic安装目录下的weblogic.properties配置文件  如自动登出时间为5分钟则修改下列参数值为5，示例如下：  weblogic.login.readTimeoutMillis=*5*  weblogic.login.readTimeoutMillisSSL=*5* |
| **检查方法** | **检查下列参数值是否符合要求**  “weblogic.login.readTimeoutMillis*”*  “weblogic.login.readTimeoutMillisSSL” |
| **依据** | 6.2.1.4 应用安全：资源控制（A3）：a) 对于有会话或短连接的应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话； |
| **备注** |  |

* + 1. 限制应用服务器Socket连接数

|  |  |
| --- | --- |
| **安全基线项目名称** | 应用服务器Socket连接数限制（按需实施） |
| **安全基线编号** | 中间件-WebLogic-7 |
| **安全基线项说明** | 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 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **参考配置操作**  以管理员身份登录管理控制台  1. 点击左侧面板的域名文件夹，然后点击Servers文件夹，双击要管理的服务器  2. 在右侧面板的“Configuration”面板下选择“Tuning”标签，查看Maximum Open Sockets值，应该配置为不大于1024 |
| **检查方法** | 要求Maximum Open Sockets的值不大于1024。 |
| **依据** | 6.2.1.4 应用安全：资源控制（A3）：b) 应能够对系统的最大并发会话连接数进行限制； |
| **备注** |  |

* 1. 其它安全项
     1. 配置错误页面处理

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置错误页面处理（必须实施） |
| **安全基线编号** | 中间件-WebLogic-8 |
| **安全基线项说明** | WebLogic错误页面重定向 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **参考配置操作**  查看<Application HOME>/WEB-INF/web.xml:文件，检查其是否包含如下片段：    如果没有则在配置文件中间部分添加此配置信息。 |
| **检查方法** | 见配置方法。 |
| **依据** | 6.2.1.4 应用安全：软件容错（A3）：c) 应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。 |
| **备注** |  |

* + 1. 禁用Send Server Header

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁用Send Server Header（建议实施） |
| **安全基线编号** | 中间件-WebLogic-9 |
| **安全基线项说明** | 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 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **参考配置操作**  以管理员身份登录管理控制台  1. 点击域名下的Servers文件夹，选择要管理的服务器  2. 在右侧面板“Protocols”面板下，点击HTTP标签  3. 检查是否勾选Send Server header |
| **检查方法** | 参照配置方法禁止勾选“Send Server header” |
| **依据** | 6.2.1.4 应用安全：软件容错（A3）：a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。 |
| **备注** |  |

* + 1. 更改默认运行端口

|  |  |
| --- | --- |
| **安全基线项目名称** | 更改默认运行端口（建议实施） |
| **安全基线编号** | 中间件-WebLogic-10 |
| **安全基线项说明** | 更改WebLogic服务器默认端口 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **参考配置操作**  查看WebLogic安装目录下的weblogic.properties配置文件，  检查weblogic.system.listenPort=*integer*（把integer改成端口号）这一项是否符合要求。 |
| **检查方法** | 检查“weblogic.system.listenPort=*”*参数值是否符合要求（自定义端口号，非默认） |
| **依据** |  |
| **备注** | 根据应用场景的不同，如部署场景需开启此功能，则强制要求此项。可能会影响系统。 |

* + 1. 配置加密协议

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置加密协议（按需实施） |
| **安全基线编号** | 中间件-WebLogic-11 |
| **安全基线项说明** | 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。 |
| **配置方法** | **版本：8.x 9.x 10.x版本**  **参考配置操作**  查看WebLogic安装目录下的weblogic.properties配置文件，请参考下列参数和参数值的配置是否符合要求：  weblogic.system.SSLListenPort=*portNumber*  weblogic.security.certificate.server=*mycert.der*  weblogic.security.key.server=*mykey.der*  weblogic.security.certificate.authority=*CA.der*  weblogic.security.certificateCacheSize=*5*  weblogic.security.clientRootCA=*anyValidCertificate*  weblogic.httpd.register.authenticated=\ weblogic.t3.srvr.ClientAuthenticationServlet  weblogic.httpd.register.T3AdminCaptureRootCA=admin.T3AdminCaptureRootCA  SSL Enabled="true" |
| **检查方法** | 见配置方法。 |
| **依据** | 6.2.1.4 应用安全：通信保密性（S3）：b) 对于通过互联网对外提供服务的系统，在通信过程中的整个报文或会话过程，应通过专用的通信协议或加密的方式保证通信过程的机密性。 |
| **备注** |  |

1. 评审与修订

本标准由老男孩定期进行审查，根据审视结果修订标准，并颁发执行。