【应用安全】浅谈 LINUX 系统 WEBSPHERE 安全配置

文/EmmaDai

0x00 WebSphere 应用介绍

WebSphere 是 IBM 的软件平台。它包含了编写、运行和监视全天候的工业强度的随需应变 Web 应用程序和跨平台、跨产品解决方案所需要的整个中间件基础设施，如服务器、服务和工具。WebSphere 提供了可靠、灵活和健壮的软件。

0x01 为什么要做安全配置

中间件 webSphere 存在安全配置不恰当导致的安全问题。webSphere 的默认配置中存在一些安全问题，例如未控制目录权限、未禁止 websphere 浏览目录等。因此，安全配置 webSphere 服务器能有效的减少安全威胁，下面将对 webSphere 安全配置进行讨论。加固方法以 webSphere 8 为例。

0x02 如何进行安全配置

1. 控制 config 与 properties 目录及子目录访问权限

要求该目录仅能 root 权限可写，一般目录设置权限 750，config 和 properties 等控制目录权限不当会导致严重后果。

加固方法：

```
cd $WAS_HOMEAppServer/<profilepath>
chown -R root config
chmod -R 750 config
chown -R root properties
chmod -R 750 properties
```

2. 禁止目录列出

禁止 WebSphere 浏览、列表显示目录。

加固方法：
编辑配置文件：
$WAS_HOME/<profilepath>/config/cells/<hostname>/applications/<yourapplication>.ear/deployments/<yourapplication>/<yourapplication>.war/WEB-INF/ibm-web-ext.xmi ，设置 directoryBrowsingEnabled="false"。

3. 禁止列表显示文件

除了禁止列出目录，同样也需要禁止 Websphere 列表显示文件。

加固方法：
编辑配置文件：
$WAS_HOME/<profilepath>/config/cells/<hostname>/applications/<yourapplication>.ear/deployments/<yourapplication>/<yourapplication>.war/WEB-INF/ibm-web-ext.xmi ，设置 fileServingEnabled="false"。

4. 启用日志

启用日志可以回溯事件进行检查或审计， 日志详细信息级别如果配置不当，会缺少必要的审计信息。

加固方法：
(1) 设置日志：
在导航窗格中，单击服务器 > 应用程序服务器-->单击您要使用的服务器的名称-->在“故障诊断”下面，单击日志记录和跟踪-->单击要配置的系统日志（诊断跟踪、 静态更改，单击“配置” 选项卡， 动态更改点击“运行时”选项卡。
(2) 设置记录级别。
在导航窗格中，单击服务器 > 应用程序服务器-->单击您要使用的服务器的名称。 在“故障诊断”下面，单击日志记录和跟踪,查看日志详细信息级别。
启用所有日志，并配置日志详细信息级别为*=info:SecurityManager=all:SystemOut=all

5. 启用全局安全性

启用全局安全性 ,控制登录管理控制台 ,同时应用程序将可以使用 WebSphere 的安全特性。

加固方法：
启用全局安全性
(1) 打开管理控制台
(2) 点击“安全性”-->”全局安全性”

6. 启用 JAVA 2 安全性

Java 2 安全性在 J2EE 基于角色的授权之上提供访问控制保护的额外级别。它特别处理系统资源和 API 的保护，不启用 Java2 安全性会极大减弱应用的安全强度。

加固方法：
启用全局安全性，如果应用程序是用 Java 2 安全性编程模型开发的，建议强制启用 Java 2 安全性。
(1) 打开管理控制台
(2) 勾选“启用全局安全性”和“强制 Java 2 安全性”

7. 配置控制台会话超时时间

控制台会话默认 30 分钟 timeout,要求设置不大于 5 分钟。

加固方法：
编辑配置文件:
$WAS_HOME/config/cells/$cell_name/applications/isclite.ear/deployments/isclite/deployment.xml，设置 invalidationTimeout=“5”。

8. 配置默认错误页面

如果没有定义默认错误网页，则当应用程序出错时会显示内部出错信息,暴露系统和应用的敏感信息。

加固方法：
编辑配置文件：
$WAS_HOME/<profilepath>/config/cells/<hostname>/applications/<yourapplication>.ear/deployments/<yourapplication>/<yourapplication>.war/WEB-INF/ibm-web-ext.xmi ， 设置 defaultErrorPage=设置为定义错误页面。

9. 卸载 sample 例子程序

sample 例子程序会泄露系统敏感信息，存在较大的安全隐患。

加固方法：
以管理员身份打开管理控制台，执行：
(1) 点击“应用程序” --> “企业应用程序”
(2) 选中例子程序， 然后点击“卸载”按钮，卸载“DefaultApplication”、“PlantsByWebSphere”、“SamplesGallery”、“ivtApp”等子程序。

0x03 总结

对 WebSphere 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