【应用安全】浅谈 LINUX 系统 TOMCAT 安全配置

文/小白

0x00 Tomcat 应用介绍

Tomcat 是 Apache 软件基金会（Apache Software Foundation）的 Jakarta 项目中的一个核心项目，由 Apache、Sun 和其他一些公司及个人共同开发而成。

Tomcat 服务器是一个免费的开放源代码的 Web 应用服务器，属于轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用，是开发和调试 JSP 程序的首选。

0x01 为什么要做安全配置

作为 web 中间件的 Tomcat 存在安全配置不恰当导致的安全问题。Tomcat 的默认配置中存在一些安全问题，例如弱密码、未禁止显示文件列表等。因此，安全配置 Tomcat 服务器能有效的减少安全威胁，下面将对 Tomcat 安全配置进行讨论。加固方法以 Tomcat 7 为例。

0x02 如何进行安全配置

1. 以非 root 用户运行 tomcat

应在普通用户的模式下，运行 tomcat 的启动脚本。查看当前系统的 tomcat 进程，程序启动时使用的身份应为非超级用户。

加固方法：
以普通用户身份运行 tomcat。

2. 修改默认端口

使用 HTTP 协议的设备，应修改 tomcat 服务器默认端口。

加固方法：
编辑 conf/server.xml 文件，修改默认端口为 xxx，重启 tomcat 服务。

```
<Connector port="xxx" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
```

3. 设置密码长度和复杂度

对于采用静态口令认证技术的设备， 口令长度应至少 8 位， 并且包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。

加固方法：
在 conf/tomcat-user.xml 文件中设置符合要求的密码，重启 tomcat 服务。

```
<user username="tomcat" password="Manager!@34" roles="">
```

4. 配置日志功能

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，以及远程登录时，用户使用的 IP 地址。

加固方法：
编辑 conf/server.xml 文件，将以下内容的注释标记取消，重启 tomcat 服务。

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
       prefix="localhost_access_log." suffix=".txt"
       pattern="common" />
```

5. 设置支持使用 HTTPS 等加密协议

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

加固方法：
1) 用 JDK 自带的工具 keytool 生成一个证书
keytool -genkey -alias tomcat -keyalg RSA -keystore /usr/local/tomcat7/conf/
（/usr/local/tomcat7/conf/为证书存放位置）
2) 编辑 conf/server.xml 文件，取消 SSL 配置的注释，并添加证书路径 keystoreFile 和密码 keystorePass 。
3) 重启 tomcat 服务。

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
           maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
                                      clientAuth="false"      sslProtocol="TLS"
keystoreFile="/usr/local/tomcat7/conf/"
           keystorePass="123456" />
```

6. 设置连接超时时间

应支持定时自动登出，自动登出时间不大于 30 秒。

加固方法：
编辑 conf/server.xml 文件，根据具体情况设置 connectionTimeout 的值，重启 tomcat 服务。

```
<Connector port="xxx" protocol="HTTP/1.1"
             connectionTimeout="20000"
             redirectPort="8443" />
```

7. 禁用 manager 功能

Tomcat 默认提供的管理页面应禁用。

加固方法：
移除 webapps 目录中的 manager 目录，禁用 manager 功能。

8. 设置错误页面重定向

Tomcat 应配置错误页面重定向，URL 地址栏中输入 http://ip:8080/manager12345 后，跳转至指向指定错误页面。

加固方法：
编辑 conf/web.xml 文件，添加或修改如下配置，重启 tomcat 服务。

```
<error-page>
<error-code>404</error-code>
<location>/noFile.htm</location>
</error-page>
……
<error-page>
<exception-type>java.lang.NullPointerException</exception-type>
<location>/error.jsp</location>
</error-page>
```

9. 禁止 tomcat 显示文件列表

应禁止 Tomcat 显示文件列表，当 WEB 目录中没有默认首页如 index.html、index.jsp 等文件时，不会列出目录内容。

加固方法：
编辑 conf/web.xml 文件，将 listings 值设置为 false，重启 tomcat 服务。

```
<init-param>
    <param-name>listings</param-name>
    <param-value>false</param-value>
</init-param>
```

10. 禁用危险的 HTTP 方法

Tomcat 应禁用 PUT、DELETE 等危险的 HTTP 方法。

加固方法：
编辑 conf/web.xml 文件，配置 org.apache.catalina.servlets.DefaultServlet 的初始化参数，将 readonly 设置为 true，重启 tomcat 服务。

```
<init-param>
    <param-name>readonly</param-name>
    <param-value>true</param-value>
</init-param>
```

11. 修改关闭 Tomcat 实例指令

应避免恶意关闭 tomcat 服务。

加固方法：
编辑 conf/server.xml 文件，将 shutdown 指令修改为复杂指令，重启 tomcat 服务。

```
<Server port="8005" shutdown="8RJbloi7kRCYniloik32UQMgbik">
```

0x03 总结

对 Tomcat 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