

河南省教育信息安全监测中心

Apache Tomcat 文件包含漏洞安全预警



河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2020 年 2 月 21 日

Apache Tomcat 文件包含漏洞安全预警

事件描述

2月20日,国家信息安全漏洞共享平台(CNVD)发布了Apache Tomcat 文件包含漏洞(CNVD-2020-10487/CVE-2020-1938)。该漏洞是由于Tomcat AJP 协议存在缺陷而导致,攻击者利用该漏洞可通过构造特定参数,读取服务器 webapp 下的任意文件。若目标服务器同时存在文件上传功能,攻击者可进一步实现远程代码执行。

影响版本

Apache Tomcat 9.x < 9.0.31

Apache Tomcat 8.x < 8.5.51

Apache Tomcat 7.x < 7.0.100

Apache Tomcat 6.x

利用风险

对于处在漏洞影响版本范围内的Tomcat而言,若其开启AJP Connector且攻击者能够访问AJP Connector服务端口的情况下,即存在被该漏洞利用的风险。

注意Tomcat AJP Connector默认配置下即为开启状态,且监听在0.0.0.0:8009。

安全建议

一、Tomcat 官方已发布 9.0.31、8.5.51 及 7.0.100 版本针对此漏洞进行修复。

二、其他修复方案

1. 如果未使用 Tomcat AJP 协议:

如果确定未使用Tomcat AJP 协议,则可以直接将Tomcat升级到9.0.31、8.5.51或7.0.100版本进行漏洞修复。而对于确定未使用Tomcat AJP 协议,但无法进行版本更新、或者是更老版本的用户,可以考虑直接关闭AJP Connector,或将其监听地址改为仅监听在本机localhost。

具体步骤:

(1) 编辑<CATALINA_BASE>/conf/server.xml,找到如下行(<CATALINA_BASE>为Tomcat的工作目录):

```
<Connector port="8009"protocol="AJP/1.3"redirectPort="8443"/>
```

(2) 将此行注释掉（或直接删掉此行）：

```
<!--<Connector port="8009"protocol="AJP/1.3"redirectPort="8443"/>-->
```

(3) 更改完毕后，重启 Tomcat 即可。

除以上措施外，当然也可以采用防火墙等办法以阻止不可信任的来源访问 Tomcat AJP-Connector 端口。

2. 如果使用了 Tomcat AJP 协议：

如果确定服务器环境中使用到了 Tomcat AJP 协议，则建议将 Tomcat 升级到 9.0.31、8.5.51 或 7.0.100 版本，同时为 AJP Connector 配置 secret 来设置 AJP 协议认证凭证。

例如（注意必须将 YOUR_TOMCAT_AJP_SECRET 更改为一个安全性高、无法被轻易猜解的值）：

```
<Connector port="8009"protocol="AJP/1.3"redirectPort="8443"  
address="YOUR_TOMCAT_IP_ADDRESS"secret="YOUR_TOMCAT_AJP_SECRET"/>
```

而对于无法进行版本更新、或者是更老版本的用户，则建议为 AJP Connector 配置 requiredSecret 来设置 AJP 协议认证凭证。例如（注意必须将 YOUR_TOMCAT_AJP_SECRET

更改为一个安全性高、无法被轻易猜解的值）：

```
<Connector port="8009"protocol="AJP/1.3"redirectPort="8443"  
address="YOUR_TOMCAT_IP_ADDRESS"requiredSecret="YOUR_TOMCAT_AJP_SECRET"  
</>
```

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052