一、漏洞公告

2020 年 2 月 4 日，Apache Tomcat 官方发布了新的版本，该版本修复了一个影响所有版本（7.*、8.*、9.*）的文件包含漏洞，但官方暂未发布安全公告，2020 年 2 月 20 日，CNVD 发布了漏洞公告，对应漏洞编号：CNVD-2020-10487，漏洞公告链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487

根据公告，Apache Tomcat 存在的文件包含漏洞能导致配置文件或源码等敏感文件被读取，建议尽快升级到漏洞修复的版本或采取临时缓解措施加固系统。

Apache Tomcat 历史安全公告请参考：

http://tomcat.apache.org/security-7.html

http://tomcat.apache.org/security-8.html

http://tomcat.apache.org/security-9.html

二、影响范围

该文件包含漏洞影响以下版本：

7.*分支 7.0.100 之前版本，建议更新到 7.0.100 版本；

8.*分支 8.5.51 之前版本，建议更新到 8.5.51 版本；

9.*分支 9.0.31 之前版本，建议更新到 9.0.31 版本。

官方下载地址：

https://tomcat.apache.org/download-70.cgi

https://tomcat.apache.org/download-80.cgi

https://tomcat.apache.org/download-90.cgi

或 Github 下载：

https://github.com/apache/tomcat/releases

三、漏洞描述

根据分析，Apache Tomcat AJP 协议不安全权限控制可通过 AJP Connector 直接操作内部数据从而触发文件包含漏洞，恶意攻击者可以通过该协议端口（默认 8009）提交攻击代码，成功利用漏洞能获取目标系统敏感文件，或在控制可上传文件的情况下执行恶意代码获取管理权限。

四、处置建议

目前，Apache 官方已发布 9.0.31、8.5.51 及 7.0.100 版本对此漏洞进行修复，建议用户尽快升级新版本或采取临时缓解措施：

1.如未使用 Tomcat AJP 协议：

如未使用 Tomcat AJP 协议，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。

如无法立即进行版本更新、或者是更老版本的用户，建议直接关闭 AJPConnector，或将其监听地址改为仅监听本机 localhost。

具体操作：

（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（也可删掉该行）：

<!--<Connectorport="8009" protocol="AJP/1.3"redirectPort="8443" />-->

（3）保存后需重新启动，规则方可生效。

2.如果使用了 Tomcat AJP 协议：

建议将 Tomcat 立即升级到 9.0.31、8.5.51 或 7.0.100 版本进行修复，同时为 AJP Connector 配置 secret 来设置 AJP 协议的认证凭证。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"/>

如无法立即进行版本更新、或者是更老版本的用户，建议为 AJPConnector 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" />