



网络安全风险预警通报

2020 年第 1 期（总第 10 期）

广西大学网络信息中心 2020 年 3 月 2 日

【预警类型】 高危预警

【预警内容】

Apache Tomcat 存在 文件包含漏洞的安全公告

安全公告编号 CNTA-2020-0004

一、漏洞概述

Tomcat 是 Apache 软件基金会 Jakarta 项目中的一个核心项目，作为目前比较流行的 Web 应用服务器，深受 Java 爱好者的喜爱，并得到了部分软件开发商的认可。Tomcat 服务器是一个免费的开放源代码的 Web 应用服务器，被普遍使用在轻量级 Web 应用服务的构架中。

攻击者利用该漏洞，可在未授权的情况下远程读取特定目录下的任意文件。目前，漏洞细节尚未公开，厂商已发布

新版本完成漏洞修复。

二、漏洞详情

Tomcat AJP 协议由于存在实现缺陷导致相关参数可控，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。若服务器端同时存在文件上传功能，攻击者可进一步实现远程代码的执行。

三、漏洞影响范围

漏洞影响的产品和版本：

Tomcat 6

Tomcat 7

Tomcat 8

Tomcat 9

四、漏洞处置建议

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，CNVD 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 AJPCoconnector，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）：

(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" />
```

附：参考链接：

[https://tomcat.apache.org/connectors-
doc/ajp/ajpv13a.html](https://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html)

[https://tomcat.apache.org/tomcat-8.0-
doc/config/ajp.html](https://tomcat.apache.org/tomcat-8.0-doc/config/ajp.html)

[https://stackoverflow.com/questions/21757694/what-
is-ajp-protocol-used-for](https://stackoverflow.com/questions/21757694/what-is-ajp-protocol-used-for)