关于 Apache Tomcat 存在文件包含漏洞的安全公告

尊敬的 CloudCC 用户，

2020 年 1 月,有机构爆出 Apache Tomcat 存在文件包含漏洞，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。目前，漏洞细节尚未公开，Tomcat 厂商已发布新版本完成漏洞修复。

此漏洞被国家信息安全漏洞共享平台（CNVD）综合评级为“高危”。

一．漏洞影响范围：

Tomcat 6

Tomcat 7

Tomcat 8

Tomcat 9

二．漏洞处理建议

如果您的 CloudCC 产品运行在以上版本的 Tomcat 环境下，请您按照以下建议进行处理：

1. 直接将 Tomcat 升级到 8.5.51 或 7.0.100 版本进行漏洞修复。
   请在 Tomcat 官方网站直接下载对应版本进行更新：
   https://tomcat.apache.org/
2. 关闭 ajp 协议，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。

   关闭方法: 找到 Tomcat 的部署安装目录，修改配置文件 conf/server.xml
   将 AJP 协议注释掉：
   <!--<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />-->

如果您已处理此 Tomcat 漏洞，可忽略上述问题，感谢您对 CloudCC 产品的支持！

北京神州云动科技股份有限公司

产品中心

2020 年 2 月 24 日