网络与信息安全情况通报

2020 年第 9 期（总第 259 期）

云南省网络与信息安全信息通报中心　　2020 年 2 月 24 日

关于 Apache Tomcat 存在文件包含漏洞的预警通报

近日，国家信息安全漏洞共享平台（CNVD）发布了关于 Apache Tomcat 存在文件包含漏洞（漏洞编号：CNVD-2020-10487、CVE-2020-1938）的预警通报。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。

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。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。Tomcat 6、7、8、9 版本均受到该漏洞的影响。

目前，Apache 官方已发布新版本对此漏洞进行了修复，

省网络与信息安全信息通报中心建议各单位用户：**一是**建议将Tomcat 升级到最新版本进行漏洞修复；**二是**如无法立即进行版本更新、或是老版本的用户，建议直接关闭 AJPConnector，或将其监听地址改为仅监听本机 localhost。

报：军号同志。

省委办公厅，省政府办公厅。

省公安厅水旺副厅长。

国家网络与信息安全信息通报中心。

送：省直各委、办、厅、局。

各重要信息系统运营使用单位及行业主管部门。

省内信息安全等级保护测评机构。

抄：省公安厅警令部，科信处，网安总队领导、各处、队。

各州、市公安局网安支队。

（共印 9 份）

审批：崔　伟　　**核稿：**张　清　　**编稿：**李健杰