漏洞预警-Apache Tomcat 远程代码执行漏洞

近期，某安全厂商监测到 Apache Tomcat 存在远程代码执行漏洞(CVE-2024-50379)，该漏洞是由于 Tomcat 在验证文件路径时存在缺陷，如果 readonly 参数被设置为 false（这是一个非标准配置），并且服务器允许通过 PUT 方法上传文件，那么攻击者就可以上传含有恶意 JSP 代码的文件。通过不断地发送请求，攻击者可以利用条件竞争，使得 Tomcat 解析并执行这些恶意文件，从而实现远程代码执行。

一、漏洞危害

高危

二、影响范围

11.0.0-M1 <= Apache Tomcat < 11.0.2

10.1.0-M1 <= Apache Tomcat < 10.1.34

9.0.0.M1 <= Apache Tomcat < 9.0.98

三、修复方式

目前官方已发布补丁，建议受影响用户尽快尽快下载安全版本修复漏洞:

官方下载链接:

11 版本：https://tomcat.apache.org/download-11.cgi

10 版本：https://tomcat.apache.org/download-10.cgi

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

修复缓解措施:

1. 在不影响业务的前提下将 conf/web.xml 文件中的 readOnly 参数设置为 true 或直接注释该参数;

2. 禁用 PUT 方法并重启 Tomcat 服务以启用新的配置。

江苏瑞新信息技术股份有限公司

2024 年 12 月 20 日