

网络安全预警信息通报

[2023]016 号

关于 Apache Tomcat 存在请求走私漏洞的 预警通报

一、基本情况

近日，通过对互联网舆情跟踪发现，Apache Tomcat 存在请求走私漏洞，由于 Tomcat 未能正确解析 HTTP Trailer 标头，可以通过特制的无效 Trailer 标头导致 Tomcat 将单个请求视为多个请求，可能导致出现请求走私。利用漏洞可能导致未授权访问敏感数据等。

Tomcat 是一个开源 Java Servlet 容器和 Web 服务器，用于运行 Java 应用程序和动态网页。

二、事件受影响范围

本次事件主要受漏洞影响的范围为：

Apache Tomcat 11.0.0-M1 - 11.0.0-M11

Apache Tomcat 10.1.0-M1 - 10.1.13

Apache Tomcat 9.0.0-M1 - 9.0.80

Apache Tomcat 8.5.0 - 8.5.93

三、安全建议

鉴于此次事件影响范围广泛、影响程度较高，因此建议采取如下措施进行安全防护：

目前官方已发布安全更新，建议升级至最新版本。

北京市政务信息安全保障中心

2023 年 10 月 12 日