安全通告

关于 Apache Tomcat 存在拒绝服务漏洞的预警通报

发布日期：2024-7-18

[2024]015 号

漏洞描述

2024 年 7 月 18 日公司监测发现，Apache Tomcat 存在拒绝服务漏洞（CVE-2024-34750），该漏洞是由于 Tomcat 在处理 HTTP/2 流时，没有正确处理某些 HTTP 标头过多的情况，导致对活跃 HTTP/2 流的计数错误，进而可能使用不正确的无限超时设置，使得本应关闭的连接保持打开状态，可能导致服务器资源消耗、性能下降和安全风险，从而造成拒绝服务。

Apache Tomcat 是一个流行的开源 Web 服务器和 Java Servlet 容器。

漏洞编号

CVE-2024-34750

漏洞危害

攻击者可能利用这一漏洞使得本应关闭的连接保持打开状态，可能导致服务器资源消耗、性能下降和安全风险，从而造成拒绝服务。

漏洞等级

高危

受影响版本

9.0.0-M1 <= Apache Tomcat <= 9.0.89

10.1.0-M1 <= Apache Tomcat <= 10.1.24

11.0.0-M1 <= Apache Tomcat <= 11.0.0

修复方案

目前官方已经发布了解决此漏洞的相关补丁，建议受影响用户升级至安全版本。

https://tomcat.apache.org/index.html

参考链接

https://lists.apache.org/thread/4kqf0bc9gxymjc2x7v3p7dvpln177y81

https://nvd.nist.gov/vuln/detail/CVE-2024-34750