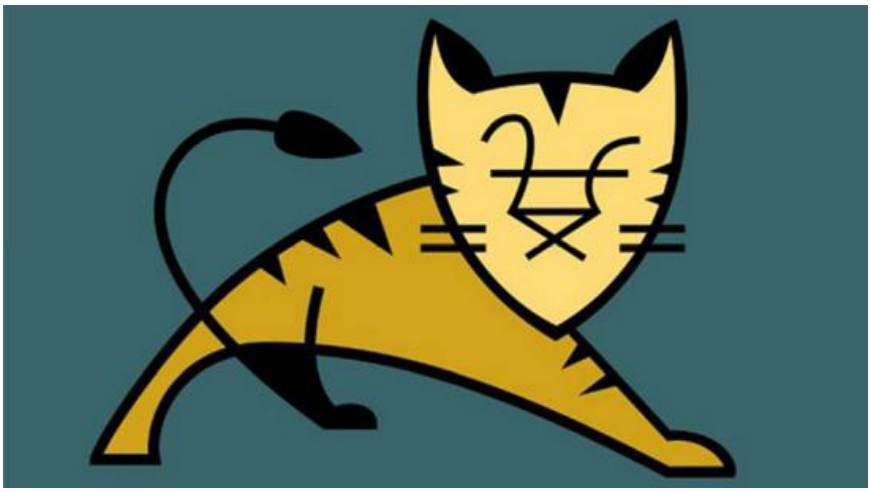
CVE-2020-11996 | Apache Tomcat HTTP/2 拒绝服务漏洞通告

0x00 漏洞概述

CVE ID	CVE-2020-11996	时 间	2020-06-29
类 型	DOS	等 级	高危
远程利用	是	影响范围	Apache Tomcat 10.0.0-M1 至 10.0.0-M5 Apache Tomcat 9.0.0.M1 至 9.0.35 Apache Tomcat 8.5.0 至 8.5.55

0x01 漏洞详情



Apache Tomcat 是美国阿帕奇（Apache）软件基金会的一款轻量级 Web 应用服务器。该程序实现了对 Servlet 和 JavaServer Page（JSP）的支持，是开发和调试 JSP 程序的首选。Apache 只支持静态网页，但像 php,cgi,jsp 等动态网页就需要 Tomcat 来处理。

2020 年 6 月 25 日，Apache 官方发布安全公告，修复了一个 Apache Tomcat 中的 HTTP/2 拒绝服务漏洞（CVE-2020-11996）。该漏洞源于恶意的 HTTP/2 请求序列可能会导致长达几秒钟的 CPU 高使用率，攻击者通过发送大量的此类请求来利用此漏洞，导致服务器拒绝响应， 从而实现 DoS 攻击。

0x02 处置建议

该漏洞影响 Apache Tomcat 10.0.0-M1 至10.0.0-M5 版本、9.0.0.M1 至9.0.35 版本和8.5.0 至 8.5.55 版本，官方已发布最新版本，请相关用户及时升级，详情如下：

1. Apache Tomcat 10.0.0-M1 至10.0.0-M5 版本的用户请升级到 10.0.0-M6 或更高版本，下载地址：https://tomcat.apache.org/download-10.cgi
2. Apache Tomcat 9.0.0.M1 至9.0.35 版本的用户请升级到 9.0.36 或更高版本，下载地址：https://tomcat.apache.org/download-90.cgi
3. Apache Tomcat 8.5.0 至8.5.55 版本的用户请升级到 8.5.56 或更高版本，下载地址：https://tomcat.apache.org/download-80.cgi

0x03 相关新闻

https://www.tenable.com/cve/CVE-2020-11996

0x04 参考链接

https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E
http://mail-archives.us.apache.org/mod_mbox/www-announce/202006.mbox/%3Cfd56bc1d-1219-605b-99c7-946bf7bd8ad4%40apache.org%3E

0x05 时间线

2020-06-25 Apache 发布安全公告
2020-06-29 VSRC 发布漏洞通告