漏洞编号: CVE-2021-30639

漏洞来源:

平台： cve/nvd

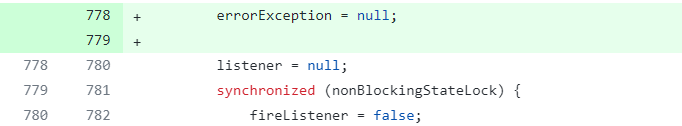
连接：https://nvd.nist.gov/vuln/detail/CVE-2021-30639

漏洞披露时间:07/26/2022

野外漏洞报告：https://cloud.tencent.com/announce/detail/1550

漏洞成因:

未能回收新添加的 errorException 对象意味着一旦aysnc 读取发生错误，所有后续异步读取都将失败。



这里原来没有及时吧errorException置空，导致异步阻塞。

漏洞PoC：无

漏洞补丁：

https://github.com/apache/tomcat/commit/b59099e4ca501a039510334ebe1024971cd6f959

漏洞类型:CWE-755 Improper Handling of Exceptional Conditions

漏洞危害:

漏洞评级：7.5HIGH

影响版本：

Tomcat:<8.5.64;

<9.0.44;10.0.3;

<10.0.4;

epolicy\_orchestrator:2.0-5.10.0

big\_data\_spatial\_and\_graph:2.0-23.1

漏洞修复版本：

Apache Tomcat >= 10.0.5  
 Apache Tomcat >= 9.0.45  
 Apache Tomcat >= 8.5.65；

epolicy\_orchestrator5.10.0之后

big\_data\_spatial\_and\_graph23.1之后

漏洞描述：

Apache Tomcat 中的漏洞允许攻击者远程发起拒绝服务攻击。这个错误是作为改进非阻塞 I/O 期间错误处理的一部分引入，意味着与 Request 对象关联的错误标志不会在请求之间重置。这意味着一旦发生非阻塞 I/O 错误，该请求对象处理的所有未来请求都将失败。用户能够触发非阻塞 I/O 错误，例如通过断开连接，从而产生触发 DoS 的可能性。不使用非阻塞 I/O 的应用程序不会暴露于此漏洞。

漏洞处置建议：

官方已发布漏洞修复版本，请评估业务是否受影响后，酌情升级至上述安全版本

漏洞参考链接：

<https://bz.apache.org/bugzilla/show_bug.cgi?id=65203>

<https://tomcat.apache.org/security-10.html>