**Apache Log4j 2远程代码执行漏洞的处理方法**

1.排查应用是否引入了Apache log4j-core Jar包，若存在依赖引入，且在受影响版本范围内，则可能存在漏洞影响。请尽快升级Apache Log4j2所有相关应用到最新的 log4j-2.15.0 版本，地址：https://logging.apache.org/log4j/2.x/download.html

2.升级已知受影响的应用及组件，如spring-boot-starter-log4j2/Apache Struts2/Apache Solr/Apache Druid/Apache Flink

3. 临时缓解方案。可升级jdk版本至6u211/7u201/8u191/11.0.1以上，可以在一定程度上限制JNDI等漏洞利用方式。对于大于2.10版本的Log4j，可设置 log4j2.formatMsgNoLookups 为True，或者将 JndiLookup 类从 classpath 中去除，例如 zip -q -d log4j-core-\*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

4. 有关Apache Log4j JMSAppender 反序列化代码执行漏洞（CVE-2021-4104）、Apache Log4j Dos漏洞（CVE-2021-45105）的临时防护措施，可参考[http://blog.nsfocus.net/apache-log4j-cve-2021-44228-cve-2021-4104-cve-2021-45046-cve-2021-45105%e5%a4%84%e7%bd%ae%e6%89%8b%e5%86%8c/](http://blog.nsfocus.net/apache-log4j-cve-2021-44228-cve-2021-4104-cve-2021-45046-cve-2021-45105%E5%A4%84%E7%BD%AE%E6%89%8B%E5%86%8C/) （绿盟科技）。