漏洞编号: CVE-2020-1948

漏洞描述:

漏洞来源: 平台 NVD

链接 https://nvd.nist.gov/vuln/detail/CVE-2020-1948

漏洞披露时间: 07/14/2020

漏洞参考链接:

野外漏洞报告：<https://cloud.tencent.com/developer/article/1653754>

漏洞类型: CWE-502

漏洞危害: 不受信任数据的反序列化

漏洞严重性:

CVSS 3.x评分：9.8

CVSS 2.0 评分：7.5

漏洞影响的组件版本:

Apache Dubbo 2.5.0 - 2.5.10 ； 2.6.0 - 2.6.7 ； 2.7.0 -2.7.4

漏洞修复的组件版本:

漏洞成因:

CVE-2020-1948远程代码执行漏洞原理是远程方法被动态调用导致的代码执行

本次漏洞利用的是 com.rometools.rome.feed.impl.ToStringBean#toString 方法，重写了 toString，该方法将会调用构造对象的所有 getter 方法

执行 Dubbo 调用时，传入的是 ToStringBean 类型参数，构造的对象是com.sun.rowset.JdbcRowSetImpl，并且 datasource 属性设置的是 JNDI 暴露的 url，在调用 JdbcRowSetImpl 的 getDatabaseMetaData 方法时，执行 connect 操作，下载远端代码，在 Service Provider 执行，造成攻击。

调起 toString 方法的地方是在 Dubbo Provider 接收 DecodeHandler#received:44 请求，在 DecodeableRpcInvocation#decode 反序列化参数的地方：

dubbo 默认使用的是 hession2 序列化，解析参数执行的是这个方法org.apache.dubbo.common.serialize.hessian2.Hessian2ObjectInput#readUTF

在 hession 反序列化过程中，通过下面代码段执行到了 ToStringBean#toString

至此，注入攻击的流程到这里执行完成。

漏洞位置:

dubbo-rpc/dubbo-rpc-api/src/main/java/org/apache/dubbo/rpc/support/RpcUtils.java

第179~180行，第183~184行

漏洞PoC：

<https://www.cnblogs.com/JingQ/p/13329083.html> 第三点就是漏洞PoC

漏洞补丁：

https://github.com/apache/dubbo/commit/5ad186fa874d9f0dfb87b989e54c1325d39abd40

漏洞处置建议：