漏洞编号: CVE-2021-43297

漏洞描述:

漏洞来源: 平台 NVD

链接 https://nvd.nist.gov/vuln/detail/CVE-2021-43297

漏洞披露时间: 01/10/2022

漏洞参考链接:

野外漏洞报告：<https://cert.360.cn/warning/detail?id=413132b068d5e062e3059adc758d3500>

这是360网络安全响应中心给出的报告，较为全面，此外还有一篇报告

<https://www.freebuf.com/articles/network/320134.html> ，对漏洞分析地比较透彻。

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 2.6.0 - 2.6.12 ； 2.7.0 - 2.7.15 ； 3.0.0 -3.0.5

漏洞修复的组件版本:

漏洞成因: Dubbo Hessian-Lite 3.2.11及之前版本中存在潜在RCE攻击风险。Hessian-Lite在遇到序列化异常时会输出相关信息，这可能导致触发某些恶意定制的Bean的toString方法，从而引发RCE攻击。这个CVE主要还是从Hessian2Input.except()->obj.toString触发的。

下面有几种触发方法：

第一种：JsonObject.toString

dubbo<=2.7.3时，由于其自带fastjson<=1.2.46版本，所以可以用JsonObject包裹一个TemplatesImpl对象，该TemplatesImpl的\_bytecodes属性携带恶意字节码，在恶意字节码实例化的过程中实现RCE，但是有版本限制

第二种：ReadOnlyBinding.toString

其实是[XBean调用链](https://github.com/threedr3am/learnjavabug/blob/master/dubbo/src/main/java/com/threedr3am/bug/dubbo/XBeanPoc.java" \t "https://www.cnblogs.com/bitterz/p/_blank)的截断，截断后的调用链如下，其实就是利用其toString方法往下调用时会用到NamingManager，在NamingManager中会去指定地址下载恶意class文件，并实例化，最终造成RCE。

<https://github.com/threedr3am/learnjavabug/blob/master/dubbo/src/main/java/com/threedr3am/bug/dubbo/XBeanPoc.java>

截断后的调用链

at java.lang.Class.newInstance(Class.java:442)

at javax.naming.spi.NamingManager.getObjectFactoryFromReference(NamingManager.java:163)

at javax.naming.spi.NamingManager.getObjectInstance(NamingManager.java:319)

at org.apache.xbean.naming.context.ContextUtil.resolve(ContextUtil.java:73)

at org.apache.xbean.naming.context.ContextUtil$ReadOnlyBinding.getObject(ContextUtil.java:204)

at javax.naming.Binding.toString(Binding.java:192)

漏洞位置:

src/main/java/com/alibaba/com/caucho/hessian/io/Hessian2Input.java第3566行；src/main/java/com/alibaba/com/caucho/hessian/io/JavaDeserializer.java第171行

漏洞PoC：<https://github.com/bitterzzZZ/CVE-2021-43297-POC>

漏洞补丁：https://github.com/apache/dubbo-hessian-lite/commit/a35a4e59ebc76721d936df3c01e1943e871729bd#

漏洞处置建议：