**漏洞报告**

漏洞编号: CVE-2021- 30179

漏洞描述:

在CVE-2021-30179中，Apache Dubbo Generic filter过滤不佳。攻击者可以构造恶意请求，调用恶意方法导致远程代码执行。

漏洞来源:

平台: CVE/NVD

链接: <https://nvd.nist.gov/vuln/detail/CVE-2021-30179>

漏洞披露时间: 06/01/2021

漏洞参考链接: 参考下面的链接

野外漏洞报告：

链接: <https://securitylab.github.com/advisories/GHSL-2021-034_043-apache-dubbo/>

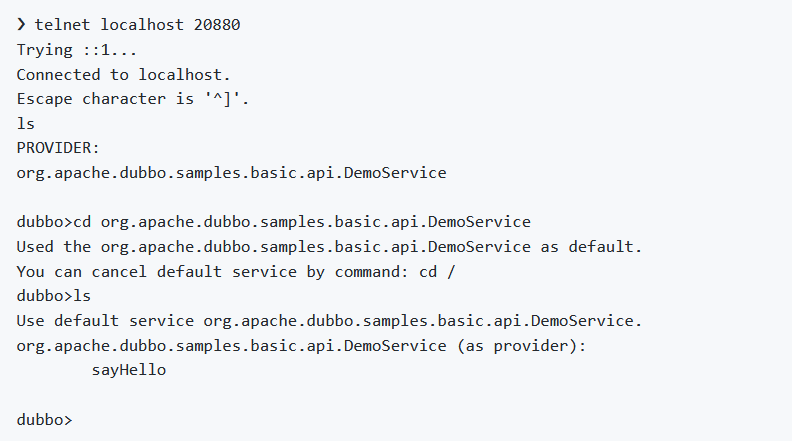
备注: 相关内容在issue4、issue5

漏洞类型: 网络远程攻击

漏洞危害:

请注意，要成功利用此问题，攻击者需要知道服务和方法名称才能访问GenericFilter代码（例如：org.apache.dubbo.samples.basic.api.DemoService和sayHello）。

通过连接到Dubbo端口并发出未经身份验证的ls命令，可以获得这些名称：



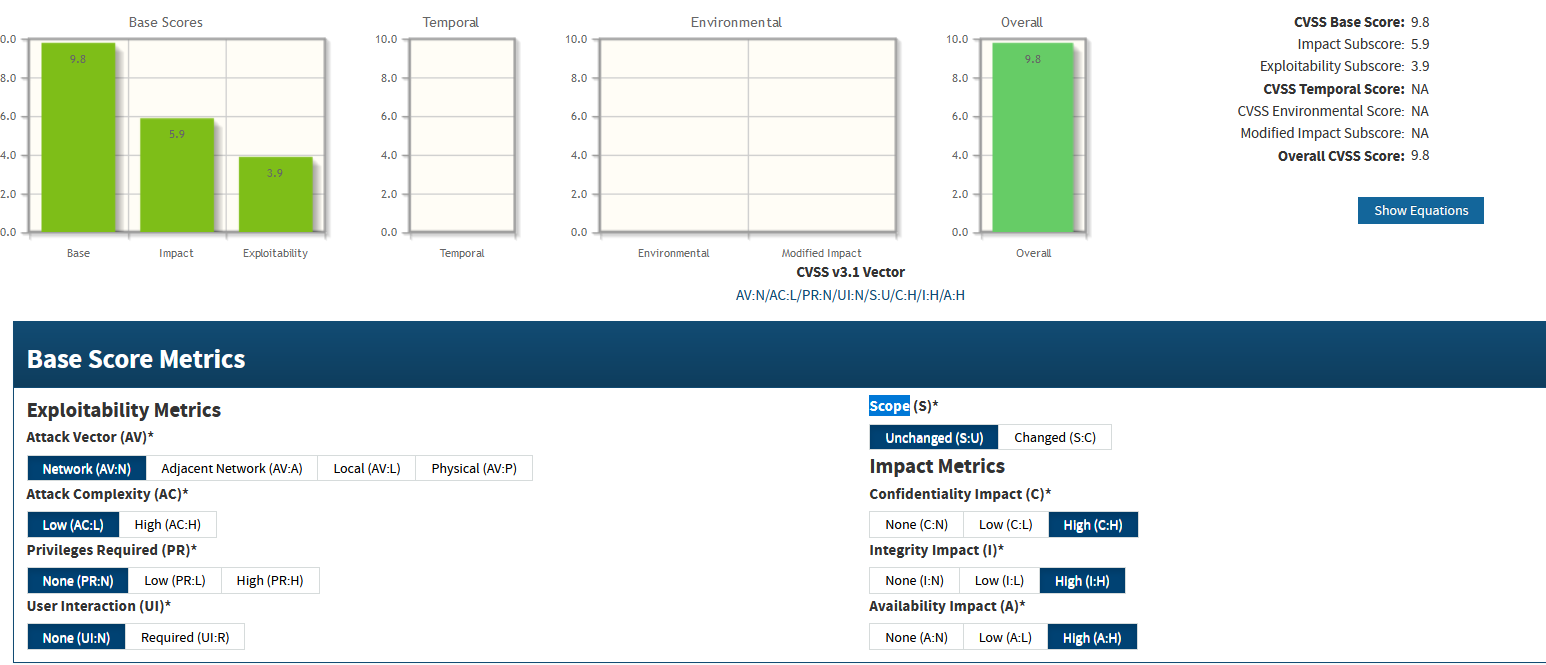
此问题可能导致预授权RCE。

在另外一种情况下，JavaBeanSerializerUtil.deserialize还允许我们调用任意类的默认构造函数，然后调用setter或为构建的对象设置字段值。例如，使用python客户端，我们可以发送以下请求，这将导致导致RCE的任意JNDI查找调用：



此问题也可能导致预授权RCE。

CVSS评分: 9.8 (已检验)



漏洞影响的组件版本:

Dubbo 2.7.0 到 2.7.9版本 (参照poc验证了2.7.9版本是有漏洞的)

在2.7.10中，使用了黑名单来阻断raw.return和bean这两条链。（参考: <https://cloud.tencent.com/developer/article/1865614> 0x04个人总结）

Dubbo 2.6.0 到2.6.9版本

Dubbo 所有 2.5.x 版本 (不再被官方维护)

漏洞修复的组件版本: 2.7.10

漏洞成因:

Apache Dubbo默认支持对提供者接口所暴露的任意方法的调用，而这些调用由GenericFilter处理，它将找到调用的第一个参数中指定的服务和方法，并使用Java Reflection API来进行最终调用。$invoke或$invokeAsync方法的签名是Ljava/lang/String;[Ljava/lang/String;[Ljava/lang/Object；其中第一个参数是要调用的方法的名称，第二个参数是包含被调用方法的参数类型的数组，第三个参数是包含实际调用参数的数组。

Apache Dubbo在处理泛类引用时，提供了多种通过反序列化方式得到对象再生成pojo对象的选择。在进行反序列化过程中没有做好防护，轻易相信用户提供的数据，直接将其进行反序列化操作，导致一些恶意对象的实例化以及相对应Gadget的触发，从而造成RCE。

漏洞位置:

参考链接: <https://cloud.tencent.com/developer/article/1865614>

文中0x03 漏洞分析部分详细展示了该漏洞的位置。

漏洞PoC：

链接: <https://cloud.tencent.com/developer/article/1865563>

漏洞补丁：N/A

备注: 阿里云漏洞库中说漏洞补丁类型是官方补丁，暂未在github上面找到

漏洞处置建议：

1. 升级 Apache Dubbo 至最新版本

2、设置 Apache Dubbo 相关端口仅对可信地址开放。