2.7.7新版本dubbo绕过说明

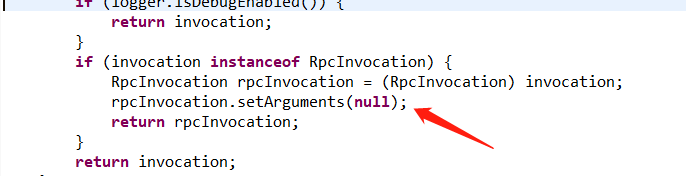
2020年6月29日dubbo针对CVE-2020-1948的补丁出现被绕过的情况。

2020年7月2日发现，dubbo删除了之前的commit修复记录，同时在最新的2.7.7代码里面增加了限制，封堵了6月29日提出的绕过的可能。

同时发现此种修复方式依然有被利用的风险。

## Dubbo修复方式分析

Dubbo的7月2日的修复方式如下图所示：



此处将传入的反射链重置为null，此处从参数的传递上有效避免了代码执行。

## 绕过方式

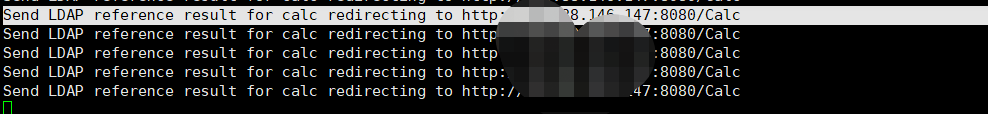
Dubbo配置开启debug日志的权限，将造成全版本的代码执行威胁，同时绕过此此版本的修复方式绕过。

log4j.rootLogger=debug, stdout

配置如上。

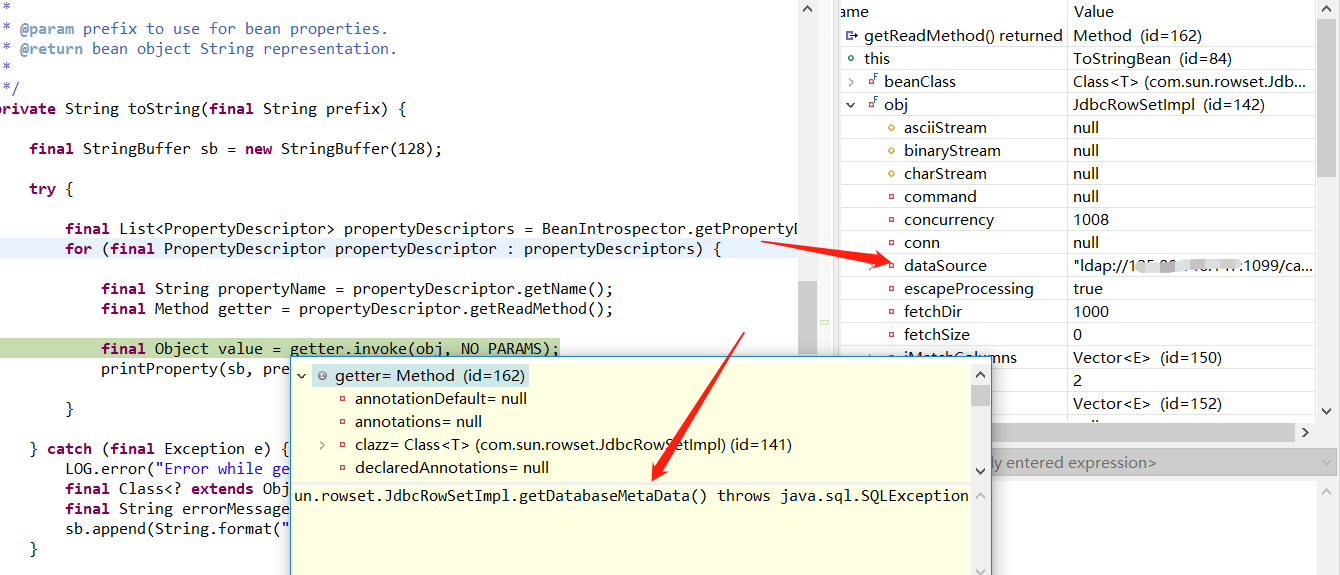
## POC证明

开启dubbo服务，利用poc测试，ldap服务器监听到ldap请求，如下图：



但是没有加载远程Calc恶意类，原因不明，但是可以确定此方式造成了代码执行，反射链问题需要再看。

漏洞触发时候，变量截图如下：



上图中动态调用反射链的getDatabaseMetData()方法，并且dataSource地址是ldap服务地址。此处造成代码执行。