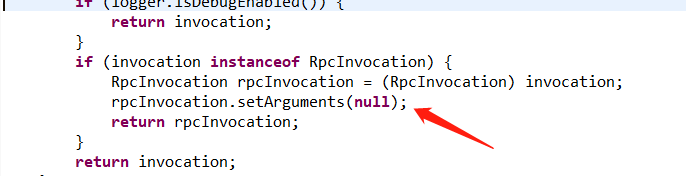
Dubbo远程代码执行说明

2020年6月29日dubbo发布新版本修复CVE-2020-1948漏洞。我们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

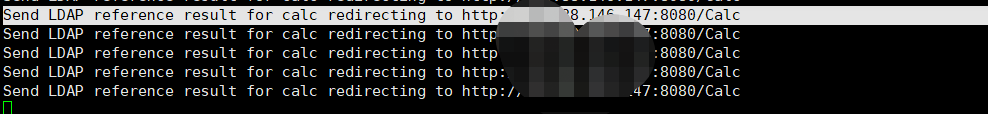
Dubbo配置开启debug日志的权限，将造成全版本的代码执行威胁，同时绕过此此版本的修复方式绕过。

log4j.rootLogger=debug, stdout

配置如上。

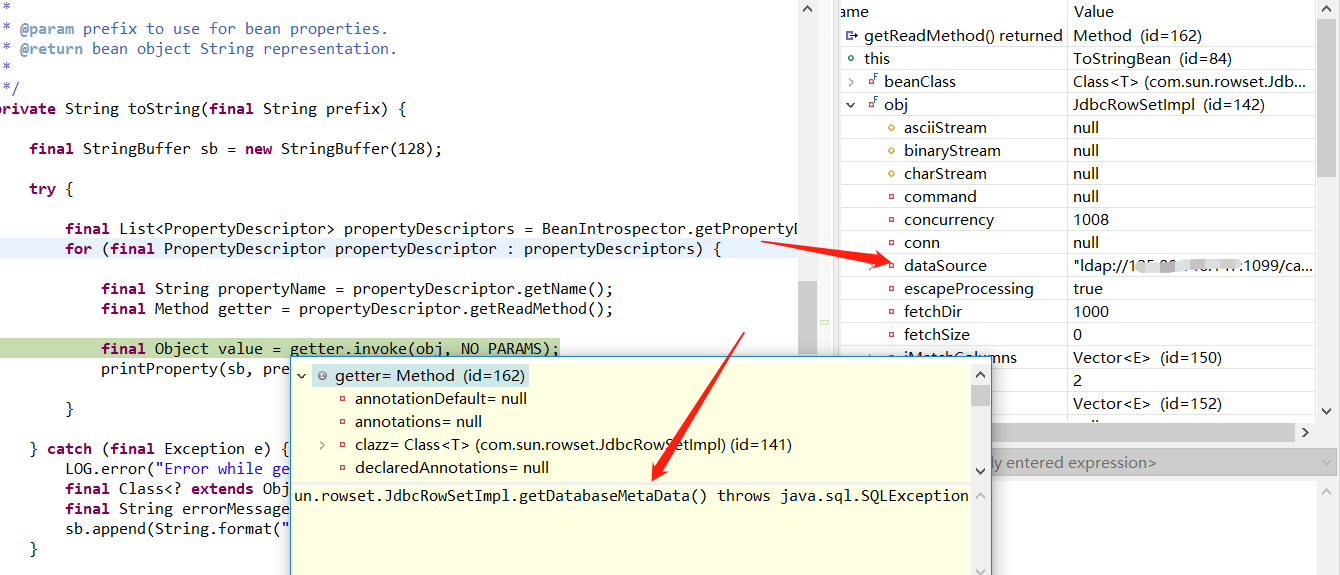
## POC证明

开启dubbo服务，利用poc测试，反射链向监听的ldap服务发送请求，ldap服务器监听到ldap请求，如下图：



此时可以确定此方式造成了代码执行。

当漏洞被触发，相关变量截图如下：



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。

执行录屏：