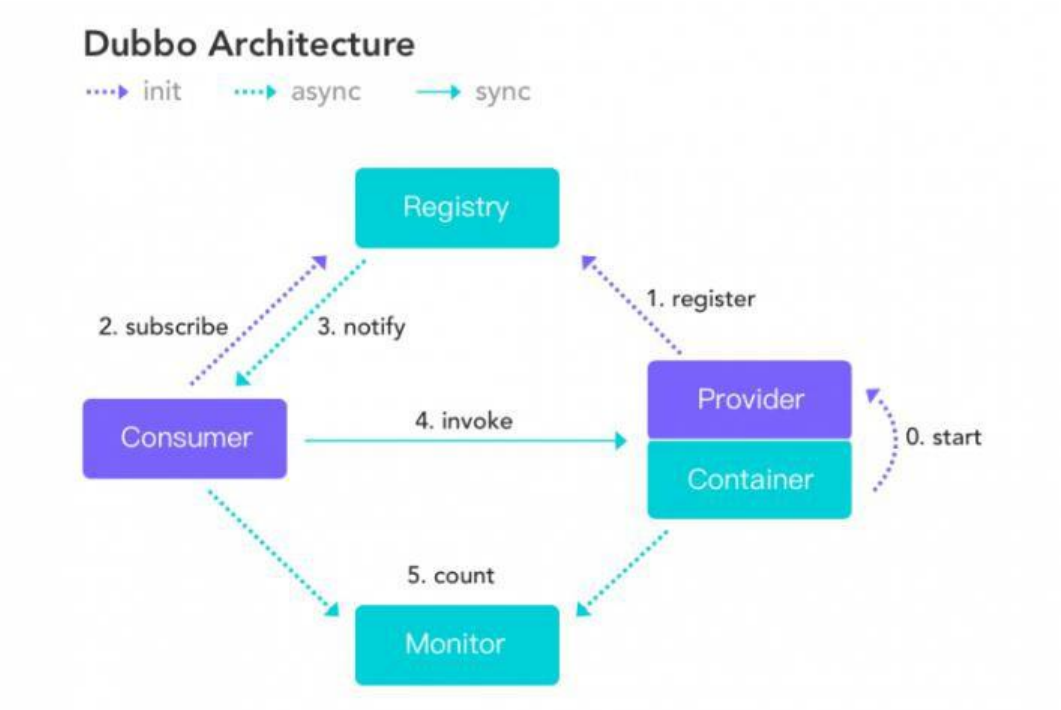
# CVE-2020-1948 | Apache Dubbo Provider 默认反序列化远程代码执行漏洞通告

## 0x00 漏洞概述

| CVE ID | CVE-2020-1948 | 时 间 | 2020-06-23 |
|---|---|---|---|
| 类 型 | RCE | 等 级 | 高危 |
| 远程利用 | 是 | 影响范围 | Dubbo 2.7.0 - 2.7.6<br>Dubbo 2.6.0 - 2.6.7<br>Dubbo 2.5.x（官方不再维护） |

## 0x01 漏洞详情




Dubbo 是阿里巴巴公司开源的一款高性能、轻量级 Java RPC 框架，它提供了三大核心能力:面向接口的远程方法调用、智能容错和负载均衡,以及自动注册服务。目前已被多家大 型企业网络采用，涉及阿里巴巴集团、中国人寿、中国电信、当当网、滴滴出行、海尔和中 国工商银行等。

2020 年 6 月 23 日 Apache 官方发布通告，修复了一个 Apache Dubbo 远程代码执行漏洞（CVE-2020-1948）。该漏洞源于 Apache Dubbo Provider 存在反序列化漏洞，攻击者可以

发送带有无法识别的服务名或方法名及某些恶意参数负载的 RPC 请求，当恶意参数被反序列化时将导致恶意代码执行。

该漏洞影响所有使用 2.7.6 或更低版本的 Dubbo 用户，漏洞等级为高危，启明星辰VSRC 建议广大用户进行资产自查，及时安装补丁。

## 0x02 处置建议

官方已发布最新版本，下载地址：
https://github.com/apache/dubbo/releases/tag/dubbo-2.7.7

升级参考文档：
http://dubbo.apache.org/zh-cn/docs/user/versions/version-270.html

注：为防止出现意外建议升级前做好数据备份。

## 0x03 相关新闻

https://meterpreter.org/cve-2020-1948-apache-dubbo-remote-code-execution-vulnerability-alert/

## 0x04 参考链接

https://lists.apache.org/thread.html/rd4931b5ffc9a2b876431e19a1bffa2b4c14367260a08386a4d461955%40%3Cdev.dubbo.apache.org%3E

## 0x05 时间线

2020-06-23 Apache 官方发布通告
2020-06-23 VSRC 发布漏洞通告