漏洞编号: CVE-2019-17564

漏洞描述:

漏洞来源: 平台 NVD

链接 https://nvd.nist.gov/vuln/detail/CVE-2019-17564

漏洞披露时间: 04/01/2020

漏洞参考链接:

野外漏洞报告：

<https://cert.360.cn/report/detail?id=fdf2dd6ab0c6e39e18a725ea86ad66bb>

<https://github.com/fairyming/CVE-2019-17564>

漏洞类型: [CWE-502](http://cwe.mitre.org/data/definitions/502.html" \t "https://nvd.nist.gov/vuln/detail/_blank)

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：6.8

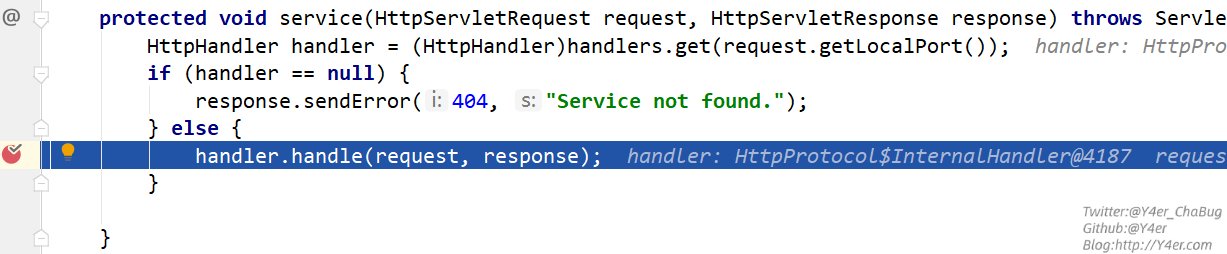
漏洞影响的组件版本:

Apache Dubbo 2.5.0 - 2.5.10 ； 2.6.0 - 2.6.7 ； 2.7.0 -2.7.4

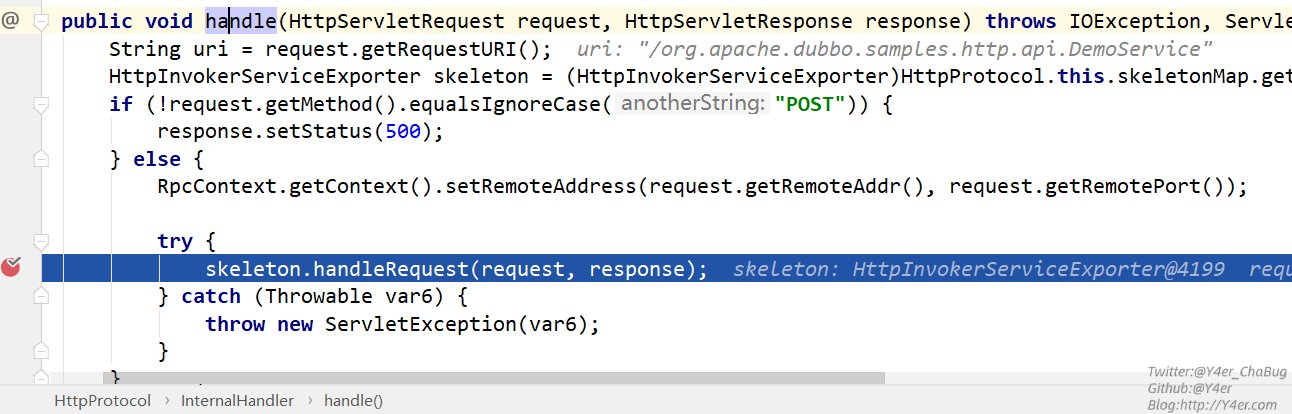
漏洞修复的组件版本:

漏洞成因:

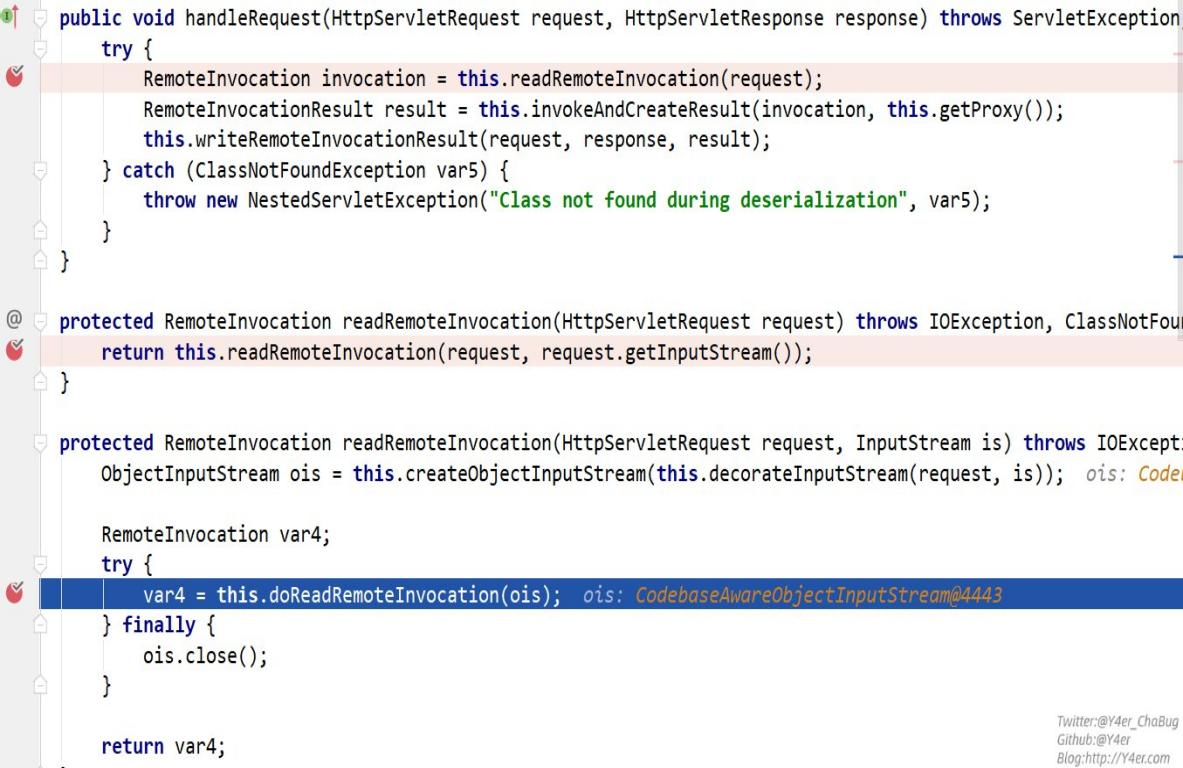
断点 dubbo-2.7.3.jar!/org/apache/dubbo/remoting/http/servlet/DispatcherServlet.class:43

[](https://y4er.com/img/uploads/20200216172086.png)

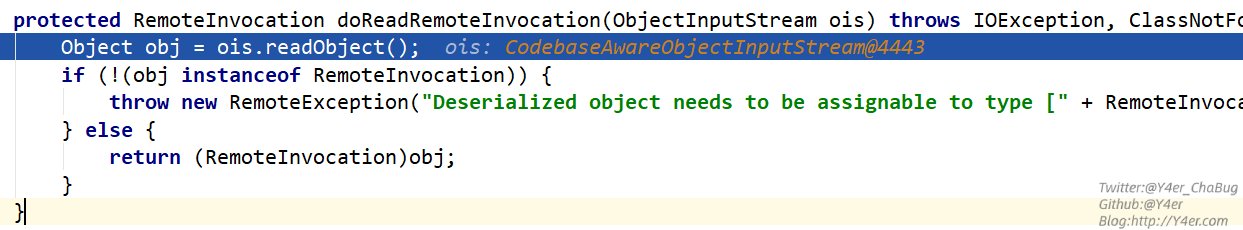
跟进到 org.apache.dubbo.rpc.protocol.http.HttpProtocol.InternalHandler#handle

[](https://y4er.com/img/uploads/20200216178969.png)

获取了URI、请求方式和RPC调用的上下文，然后进入handleRequest()

[](https://y4er.com/img/uploads/20200216173990.png)

handleRequest()将request请求对象传入一个参数的readRemoteInvocation()，然后将request和request.getInputStream()传入其重载方法两个参数的readRemoteInvocation()，然后创建了ois对象，ois对象中包含了post请求的数据，然后进入doReadRemoteInvocation()

[](https://y4er.com/img/uploads/20200216177168.png)

到达readObject()，整个过程ois对象没有过滤，而ois中又包含了post报文，导致反序列化漏洞，如果存在可用的gadget，会导致RCE。

漏洞位置:

org.springframework.remoting.rmi.RemoteInvocationSerializingExporter#doReadRemoteInvocation第68行

漏洞PoC：

http://www.code2sec.com/cve-2019-17564-dubbo-httpxie-yi-fan-xu-lie-hua-lou-dong.html

漏洞补丁：https://github.com/apache/dubbo/commit/5e2c07c1dc3f945c6375cbeb021af30fa6d4ac31

漏洞处置建议：