# 漏洞报告

###### 漏洞编号

CVE-2021-25641

###### 漏洞描述

每个Dubbo服务器都会设置一个序列化ID，告诉客户端它正在使用哪个序列化协议。但是对于 2.7.8 或 2.6.9 之前的 Dubbo 版本，攻击者可以通过篡改字节序码标志（即不遵循服务器的指令）来选择提供程序将使用的序列化 ID。这意味着，如果弱反序列化程序（如 Kryo 和 FST）以某种方式在代码范围内（例如，如果 Kryo 在某种程度上是依赖项的一部分），则未经身份验证的远程攻击者可以告诉提供程序使用弱反序列化程序，然后继续利用它。

###### 漏洞来源

平台:CVE/NVD 链接: [NVD - CVE-2021-25641 (nist.gov)](https://nvd.nist.gov/vuln/detail/CVE-2021-25641)

###### 漏洞披露时间

2021-06-01

###### 漏洞参考链接

阿里云：[【Dubbo安全漏洞通告】-CVE-2021-25641-Hessian2协议反序列化漏洞 (aliyun.com)](https://help.aliyun.com/document_detail/268280.html)

漏洞通告：[【漏洞通告】Apache Dubbo漏洞通告 (CVE-2021-25641/CVE-2021-30181) | CN-SEC 中文网](http://cn-sec.com/archives/383314.html)

漏洞复现：[Dubbo的反序列化安全问题——kryo和fst - bitterz - 博客园 (cnblogs.com)](https://www.cnblogs.com/bitterz/archive/2021/11/22/15588955.html)

###### 野外漏洞报告

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

备注: CVE-2021-25641对应的编号为GHSL-2021-035 ，在报告中所对应的位置为Issue 2: Bypass Hessian2 allowlist via alternative protocols (GHSL-2021-035)

###### 漏洞类型

CWE-502

###### 漏洞危害

攻击者可利用其他协议绕过Hessian2黑名单造成反序列化

###### 漏洞严重性

CVSS Version 3.x: 9.8 CRITICAL, CVSS Version 2.0: 7.5 HIGH

###### 漏洞影响的组件版本

dubbo:[2.5.0,2.6.9), [2.7.0,2.7.8)

###### 漏洞修复的组件版本

dubbo: 2.7.3及以上版本

###### 漏洞成因

虽然hessian2协议通过允许列表限制了反序列化的内容，但是其他反序列化协议没有被这样保护。在RPC请求头指定的序列化协议可以是任意一个以下的协议。

2 -> "hessian2"

3 -> "java"

4 -> "compactedjava"

6 -> "fastjson"

7 -> "nativejava"

8 -> "kryo"

9 -> "fst"

10 -> "native-hessian"

11 -> "avro"

12 -> "protostuff"

16 -> "gson"

21 -> "protobuf-json"

22 -> "protobuf"

25 -> "kryo2"

为了防止攻击者强制执行native Java反序列化，服务器会检查序列化Id，如果攻击者要求执行服务器未配置的反序列化，应用会抛出异常。但是攻击者可以要求运行其余的协议，并且这些协议大多没有受到保护，会导致远程代码执行。

漏洞位置: 代码位置（文件+函数+代码行数）

###### 漏洞PoC

[CVE-2021-25641-Proof-of-Concept/DubboProtocolExploit at main · Dor-Tumarkin/CVE-2021-25641-Proof-of-Concept (github.com)](https://github.com/Dor-Tumarkin/CVE-2021-25641-Proof-of-Concept/tree/main/DubboProtocolExploit)

###### 漏洞补丁

链接：[Add serialize id check for 2.6 (#7912) · apache/dubbo@077da34 (github.com)](https://github.com/apache/dubbo/commit/077da34addab54d9718710f6848669c4f0d701f1)

###### 漏洞处置建议

1. 升级Dubbo版本
2. 配置环境变量serialization.security.check=true，开启强校验。