# 漏洞报告

###### 漏洞编号

CVE-2021-30180

###### 漏洞描述

Apache Dubbo 2.7.9 之前的版本支持标签路由，这将使客户能够将请求路由到正确的服务器。客户在发出请求时使用这些规则来查找正确的终结点。在解析这些 YAML 规则时，Dubbo 客户可以启用调用任意构造函数。

###### 漏洞来源

平台：CVE/NVD 链接：[NVD - CVE-2021-30180 (nist.gov)](https://nvd.nist.gov/vuln/detail/CVE-2021-30180)

###### 漏洞披露时间

06/01/2021

###### 漏洞参考链接

[【安全通报】Apache Dubbo 多个预认证 RCE 漏洞（CVE-2021-25641等）|NOSEC安全讯息平台 - 白帽汇安全研究院](https://www.nosec.org/home/detail/4778.html)

[Apache Dubbo漏洞跟进研究 - 唐小风 - 博客园 (cnblogs.com)](https://www.cnblogs.com/suyu7/p/14928710.html)

[Apache Dubbo相关漏洞复现 | CN-SEC 中文网](https://cn-sec.com/archives/406069.html)

###### 野外漏洞报告

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

备注: 对应编号及位置 GHSL-2021-040 (7), GHSL-2021-041 (8), GHSL-2021-043(10)

###### 漏洞类型

CWE-444

###### 漏洞危害

Apache Dubbo多处使用了yaml.load，从而造成了Yaml反序列化漏洞。

###### 漏洞严重性

CVSS 3.x：9.8 CRITICAL，CVSS 2.0：6.8 MEDIUM

###### 漏洞影响的组件版本

dubbo:[2.7.0, 2.7.10)

###### 漏洞修复的组件版本

2.7.10-2.7.15

###### 漏洞成因

Apache Dubbo多处使用了yaml.load，攻击者在控制如ZooKeeper注册中心后可上传恶意配置文件从而造成了Yaml反序列化漏洞。

###### 漏洞位置

[dubbo/TagRuleParser.java at f4b225eb3a5acdf7c9064763f522ea0b86421c8d · apache/dubbo (github.com)](https://github.com/apache/dubbo/blob/f4b225eb3a5acdf7c9064763f522ea0b86421c8d/dubbo-cluster/src/main/java/org/apache/dubbo/rpc/cluster/router/tag/model/TagRuleParser.java" \l "L35-L36)

35-36行

###### 漏洞PoC

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

###### 漏洞补丁

[Use safeConstructor instead of constructor when parsing yaml by kevinw66 · Pull Request #7437 · apache/dubbo (github.com)](https://github.com/apache/dubbo/pull/7437/commits/4b7f533547da91f9839bda41fc5a1d04c18c415c)

1. 漏洞处置建议：升级至2.7.10及以上版本
2. 修改代码补丁<https://github.com/apache/dubbo/pull/7437/commits/4b7f533547da91f9839bda41fc5a1d04c18c415c#diff-28e28582e4518342f09625d18879b4f7cee960496bd04863eb187064d030372f>