安全漏洞通告

Apache Dubbo 多个高危漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	Apache Dubbo 多个高危漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-062402
报告版本	1	报告日期	2021-06-24
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-06-24	360CERT	360CERT	撰写报告

目录

1 漏洞简述 4
2 风险等级 5
3 漏洞详情 6
CVE-2021-25641: Dubbo 序列化漏洞 6
CVE-2021-30179: Dubbo 验证绕过漏洞 6
CVE-2021-32824: Dubbo 验证绕过漏洞 6
CVE-2021-30180: Dubbo 序列化漏洞 7
CVE-2021-30181: Dubbo 代码执行漏洞 7
4 影响版本 8
5 修复建议 9
通用修补建议 9
6 相关空间测绘数据 10
7 时间线 11
8 参考链接 12
附录 13
A 产品侧解决方案 13
360 城市级网络安全监测服务 13
360 安全分析响应平台 13
360 本地安全大脑 14
360 终端安全管理系统 14

B 报告等级说明 16
严重 16
高危 16
中危 17
低危 18
C 影响面说明 20
D 360CERT 内部评分体系 21

1 漏洞简述

2021 年 06 月 24 日，360CERT 监测发现 GithubSecurityLab 发布了 Dubbo组件多个高危漏洞 的风险通告，漏洞编号为 CVE-2021-25641等 ，漏洞等级：高危，漏洞评分：8.5。

ApacheDubbo 是一款高性能、轻量级的开源JavaRPC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，以及服务自动注册和发现。

漏洞的相关技术细节已由 Github SecurityLab 公开。

对此，360CERT 建议广大用户及时将 ApacheDubbo 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

2 风险等级

360CERT 对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	广泛
攻击者价值	高
利用难度	高
360CERT 评分	8.5

3 漏洞详情

3.1 CVE-2021-25641: Dubbo 序列化漏洞

CVE: CVE-2021-25641

组件: Dubbo

漏洞类型: 序列化漏洞

影响: 代码执行, 服务器接管

简述: Apache Dubbo 因支持 Hessian2 序列化框架，攻击者利用特制的数据包绕过 Hessian2 黑名单限制，实现任意代码执行。

3.2 CVE-2021-30179: Dubbo 验证绕过漏洞

CVE: CVE-2021-30179

组件: Dubbo

漏洞类型: 验证绕过漏洞

影响: 代码执行, 服务器接管

简述: Apache Dubbo Generic filter 存在过滤不严，攻击者可构造恶意请求调用恶意方法从而造成任意代码执行。

3.3 CVE-2021-32824: Dubbo 验证绕过漏洞

CVE: CVE-2021-32824

组件: Dubbo

漏洞类型: 验证绕过漏洞

影响: 代码执行, 服务器接管

简述: Apache Dubbo Telnet handler 在处理相关请求时，允许攻击者调用恶意方法

从而造成远程代码执行。

3.4 CVE-2021-30180: Dubbo 序列化漏洞

CVE: CVE-2021-30180
组件: Dubbo
漏洞类型: 序列化漏洞
影响: 代码执行, 服务器接管
简述: Apache Dubbo 使用了 yaml.load 从外部加载数据内容及配置文件，攻击者在控制如 ZooKeeper 注册中心后可上传恶意配置文件，然后通过 Dubbo 调用 RPC 加载该配置文件从而造成了 Yaml 反序列化，实现任意代码执行。

3.5 CVE-2021-30181: Dubbo 代码执行漏洞

CVE: CVE-2021-30181
组件: Dubbo
漏洞类型: 代码执行
影响: 服务器接管
简述: Apache Dubbo 在和 ZooKeeper 进行协同通信的过程中存在漏洞，攻击者在控制如 ZooKeeper 注册中心后可构造恶意请求注入 Nashorn 脚本，造成任意代码执行。

4 影响版本

影响组件	影响版本	安全版本
Apache:Dubbo	< 2.6.10,	2.6.10
Apache:Dubbo	< 2.7.10	2.7.10
Apache:Dubbo	2.5.*	2.7.10

5 修复建议

5.1 通用修补建议

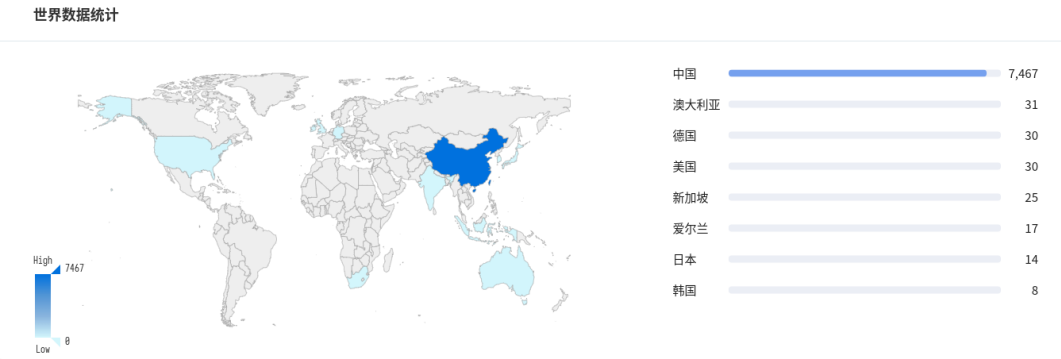
根据 安全版本 前往 Github 下载更新 Release

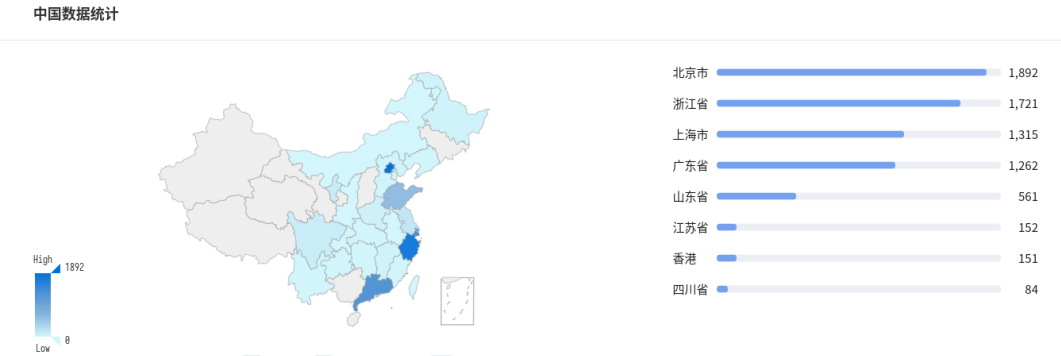
apache/dubbo Github Release

6 相关空间测绘数据

360 安全大脑-Quake 网络空间测绘系统通过对全网资产测绘，发现 Dubbo ，具体分布如下图所示。

Quake 搜索表达式: app:"Apache_Dubbo"





7 时间线

2021-06-22 Github SecurityLab 发布通告

2021-06-22 Github SecurityLab 发布通告

2021-06-24 360CERT 发布通告

8 参考链接

GHSL-2021-034_043: Multiple pre-auth RCEs in Apache Dubbo

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或 (quake#360.cn) 获取对应产品。

A.2 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或 (shaoyulong#360.cn) 获取对应产品。

A.3 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

A.4 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全

产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

B 报告等级说明

360CERT 评分是依托于 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 实施攻击成本低，难度低 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 (a) 占用存储空间 (b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

C 影响面说明

影响面说明	
广泛	1. 影响主体数 > 10w 2. 底层依赖库
一般	1. 5w < 影响主体数 < 10w 2. 次级开源库
局限	1. 影响主体数 < 5w 2. 特制版本的

D 360CERT 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 –10.0	严重
7.0 –8.9	高危
4.0 –6.9	中危
0 –3.9	低危