**漏洞报告**

漏洞编号: CVE-2021- 36161

漏洞描述:

Dubbo中的一些组件会尝试打印输入参数的格式化字符串，这有可能会对带有特殊toString方法的恶意定制bean造成RCE。在最新版本中，我们修复了超时、缓存和其他一些地方的toString调用。在Apache Dubbo 2.7.13中得到修正。

漏洞来源:

平台: CVE/NVD

链接: <https://nvd.nist.gov/vuln/detail/CVE-2021-36161>

漏洞披露时间: 09/09/2021

漏洞参考链接: N/A

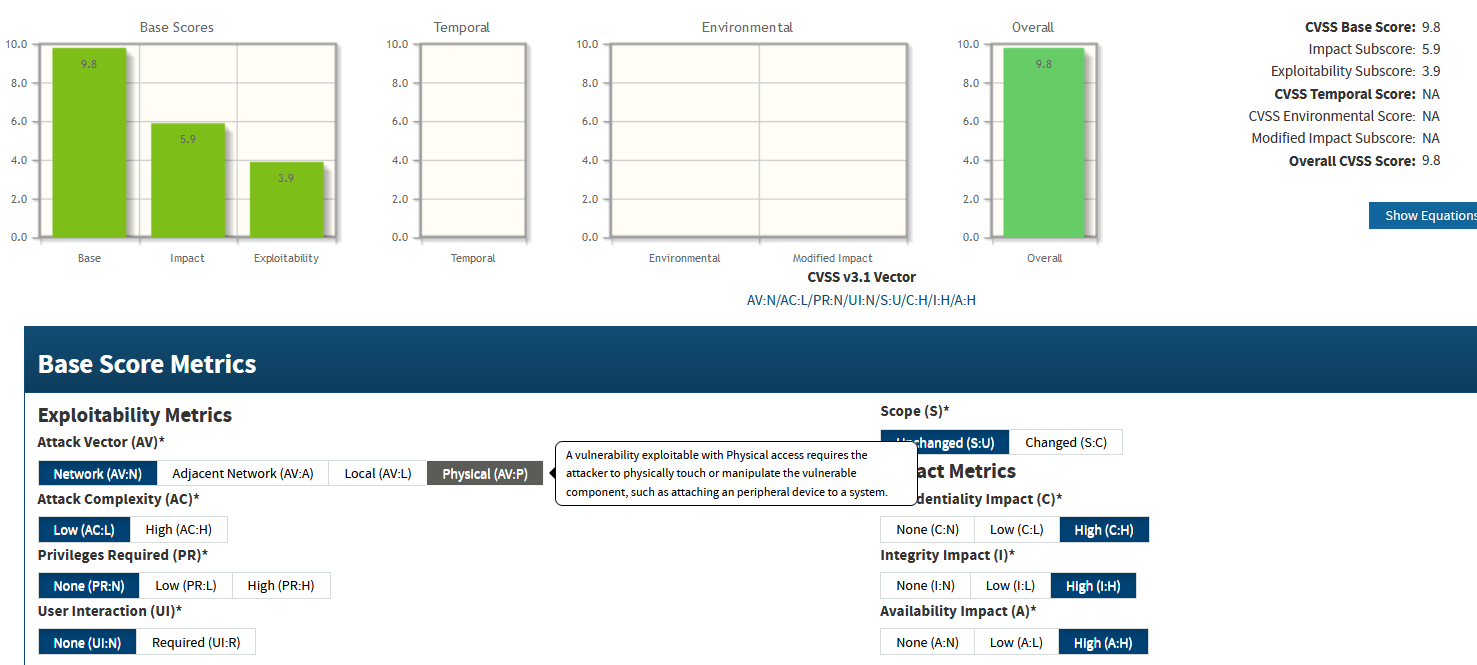
野外漏洞报告:

链接: <https://help.aliyun.com/document_detail/309540.html>

漏洞类型: 网络远程攻击漏洞

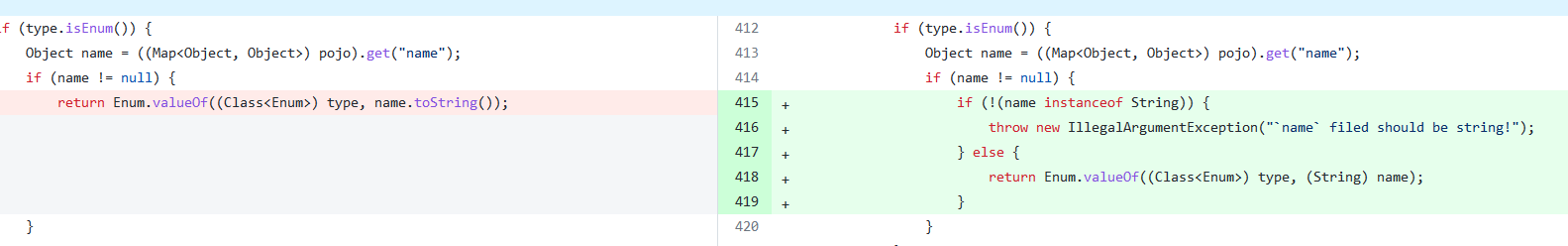
漏洞严重性: 可能会造成RCE、代码执行等，可能会通过注入非法字符串来触发。

CVSS评分: 9.8 (已检验)



漏洞影响的组件版本:

Duddo 2.7.0到2.7.12



经检验，在2.7.13版本之前的都没有对toString函数有相关的处理。

漏洞修复的组件版本: 2.7.13

漏洞成因: 此漏洞会影响 toString的正常使用。手动调试的不合法输入可导致 Format String。 使用CWE来说明的话，就是这个漏洞会导致 [CWE-134](https://vuldb.com/zh/?vulnerability_cwe.182308) 问题的产生。

漏洞位置: 根据补丁我们可以推出漏洞在dubbo-common/src/main/java/org/apache/dubbo/common/utils/PojoUtils.java

文件中

漏洞PoC：N/A

漏洞补丁：

链接: <https://github.com/apache/dubbo/commit/d16d0e15d8ffbf9b06c92639559f59dc29ddb42f>

备注: 软件在2.7.13版本解决了这个漏洞。

漏洞处置建议：

将Duddo软件更新到2.7.13以上的版本。